LE PARI ÉTALE

par

A. C.

Résumé. — Ces notes sont une transcription des notes de mon exposé. L'objectif était de discuter de la construction de la cohomologie étale.

Table des matières

Introduction

L'objectif de cet exposé était de présenter la construction d'une théorie cohomologique qui a joué un rôle crucial dans la preuve des conjectures de Weil. Je souhaitais surtout expliquer (pour ce que j'en comprends) comment, partant du cadre « topologique » par exemple celui des variétés algébriques complexes dans lequel on peut introduire des invariants naturels tels que le *groupe fondamental* ou les *groupes d'homologie simpliciale*, on est parvenus à développer des constructions « analogues » s'adaptant à un cadre nettement plus hostile, celui des variétés sur des corps finis.

1. Quelques motivations

1.1. Pourquoi ? — On peut se demander pourquoi j'ai eu envie de vous raconter ça. Il est d'ailleurs important de préciser dès maintenant que je ne suis pas un spécialiste du sujet et je tiens d'ailleurs à m'excuser si certains éléments qui vont suivre peuvent sembler approximatifs. Comme je le disais dans l'introduction, j'ai surtout souhaité retranscrire la compréhension que j'ai pu me développer de ces objets. Je n'aurais pour autant pas la prétention de dire que je les maîtrise en profondeur.

Donc, pourquoi vous parler de cohomologie étale ? D'abord parce que étudiant j'étais passionné par la topologie. Ensuite, en thèse j'ai travaillé sur des codes correcteurs d'erreurs construits à partir de variétés sur des corps finis. Si la géométrie algébrique sur des corps finis a quelque chose de passionnant, je conservais cette nostalgie de mes cours de topologie algébrique. Un jour, on m'a dit « bah sur les corps finis, la cohomologie étale c'est un peu la même chose que la cohomologie singulière pour les variétés complexes ». Ça m'a donné envie d'aller voir cela de plus près.

Pour les références, j'ai surtout beaucoup appris des notes de cours de Milne [**9**] que je trouve formidables. Son livre [**8**] permet d'aller plus loin.

1.2. Parlons peu mais parlons de moi. — Ma recherche porte sur sur la théorie des codes d'une part et la cryptographie d'autre part. Dans les mathématiques qui sont derrière, beaucoup de corps finis et de polynômes en une ou plusieurs variables. Dans ce monde, un problème récurrent consiste à borner supérieurement ou inférieurement le nombre de solutions à coordonnées dans un corps $\mathbb{F}_q$ d'un système d'équations polynomiales. Géométriquement parlant, borner le nombre de points à coordonnées dans $\mathbb{F}_q$ d'une variété algébrique.

Pour ne pas rester éternellement dans le flou, commençons par donner un exemple, celui de la *distance minimale* des *codes géométriques*. Pour qu'une information puisse être communiquée via un canal bruité puis récupérée sans perte à l'autre bout de la chaîne, on utilise des *codes correcteurs d'erreurs*. Un code correcteur d'erreurs est un sous-espace $\mathscr{C}$ de dimension $k < n$ de $\mathbb{F}_q^n$ que l'on munit de la métrique de *Hamming* :

$$\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n,\ d_H(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \sharp\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}.$$

On peut vérifier que cette fonction vérifie les propriétés qui définissent une distance (symétrie, séparation, inégalité triangulaire). Cette métrique est par ailleurs naturelle : un vecteur perturbé, *i.e.* dont un « petit » nombre de coordonnées auront été modifiées sera proche du vecteur d'origine. L'idée centrale des codes correcteurs est que pour pouvoir communiquer via un canal bruité, il faut transmettre une information redondante : un message de k symboles sera encodé en un message de n symboles via une application d'*encodage* $\mathrm{enc} : \mathbb{F}_q^k \xrightarrow{\sim} \mathscr{C} \subset \mathbb{F}_q^n$. À la sortie, le processus est efficace si l'on est capable à partir d'un vecteur $\mathbf{y}'$ proche d'un élément $\mathbf{y}$ de $\mathscr{C}$ de retrouver $\mathbf{y}$. Cette procédure appelée *décodage* est pour le moins complexe et je n'en parlerai pas ici. Je me limiterai à cette remarque : il sera d'autant plus difficile de décoder que les éléments de $\mathscr{C}$ sont proches les uns des autres. Aussi, il est naturel d'introduire la *distance minimale* de $\mathscr{C}$, qui est la plus petite distance de Hamming possible entre deux éléments distincts de $\mathscr{C}$. Du fait de la discussion qui précède, il est souhaitable que cette quantité soit la plus grande possible. Il s'avère que le calcul de la distance minimale d'un code est un problème difficile d'un point de vue algorithmique [**1**]. Cependant, pour certaines constructions, ce calcul se ramène à un problème géométrique que l'on sait plus ou moins facilement résoudre.

Une première construction est celle de Reed–Solomon :

$$\mathscr{C} = \{(f(x_1), \dots, f(x_n)) \mid f \in \mathbb{F}_q[X],\ \deg f < k\}.$$

Autrement dit, chaque vecteur du code s'obtient comme évaluation multiple d'un même polynôme en des valeurs distinctes $x_1, \dots, x_n \in \mathbb{F}_q$. Par linéarité, calculer la distance minimale du code revient à calculer la distance minimale au vecteur nul, ce qui revient à compter le nombre minimal de coefficients non nuls d'un vecteur, ce qui équivaut à estimer le nombre maximal de coefficients nuls. Cette dernière quantité est bornée par le nombre de racines du polynôme, lui-même borné par son degré. On trouve ainsi une borne inférieure pour la distance minimale : $d \geqslant n - k + 1$.

Si l'on souhaite faire grandir n, les x_i devant être distincts (sinon le raisonnement sur la distance minimale devient faux), on est rapidement bloqués par la taille du corps. La solution proposée par Goppa au début des années 80 est de remplacer $x_1, \dots, x_n$ par les points d'une courbe et d'évaluer des fonctions rationnelles sur cette courbe. Cette construction des codes dits *géométriques* généralise la première (les codes de Reed–Solomon pouvant être vus comme des codes géométriques associés à la droite) et une borne sur la distance minimale de tels codes s'obtient par des arguments très similaires : une borne supérieure sur le nombre maximal de zéros d'une fonction non nulle vivant dans un certain espace. Voir par exemple, [**10**] pour une introduction accessible aux codes à partir de courbes.

Arrive l'étape suivante : et si on remplaçait « courbe » par une surface ou une variété de dimension supérieure ? On peut toujours construire notre code par évaluation de fonctions en des points de cette variété, mais la distance minimale devient bien plus ardue à évaluer. Pour le comprendre, commençons par prendre la courbe la plus simple possible : la droite et la variété de dimension supérieure la plus simple possible : le plan. Les fonctions « naturelles » sur la droite sont les polynômes en une variable et une telle fonction a un nombre fini de racines, même

sur un corps infini. Si l'on passe au plan, les fonctions naturelles sont les polynômes en deux variables et ces dernières ont un lieu d'annulation qui, sur un corps algébriquement clos, est infini. Autrement dit, les zéros d'un polynôme non nul en une variable forment un ensemble fini : il est de dimension nulle, alors que ceux d'un polynôme en deux variables forment une courbe : un ensemble algébrique de dimension 1. Ce fait se généralise naturellement aux courbes et variétés de dimension quelconque. Sur une courbe, le lieu d'annulation d'une fonction est de dimension nulle et son cardinal peut être borné *indépendamment du corps de base*. Si par contre on considère une fonction sur une surface, ses zéros forment une courbe et la question ne va plus être de borner le nombre zéros (qui sur la clôture algébrique du corps de base est infini) mais de borner le nombre de points à coordonnées dans $\mathbb{F}_q$ de ce lieu des zéros (qui, rappelons le, est une courbe tracée sur la surface).

Le problème est d'autant plus complexe qu'il ne s'agit pas de le résoudre pour une seule fonction (et donc pour une seule courbe) mais bien pour toutes les fonctions d'un espace donné. Ce qui motive à chercher des bornes supérieures sur le nombre de points de courbes appartenant à une famille et donc à avoir des bornes ne dépendant que de certains invariants associés à la courbe. Pour plus de détails, je renvoie à [**5**] qui traite le cas des paramètres de codes sur un espace projectif et à [**6**] pour un *survey paper* sur les codes à partir de variétés de dimension supérieure à 2.

1.3. Les conjectures de Weil. — On entre alors en plein dans le vif du sujet : comment compter le nombre de points à coordonnées dans $\mathbb{F}_q$ d'une courbe ou d'une variété de dimension supérieure ?

Étant donnée une variété V sur un corps fini, on la munit de l'endomorphisme de Frobenius qui envoie un point $(x_1, \ldots, x_t)$ sur $(x_1^q, \ldots, x_t^q)$. C'est un endomorphisme de V dont les points fixes sont précisément les points à coordonnées dans $\mathbb{F}_q$. En géométrie complexe, on connait de longue date la formule dite *des traces de Lefschetz* qui permet de déterminer le nombre de points fixes d'un endomorphisme sur une variété en fonction de la manière dont il agit sur ses groupes de cohomologie singulière. La folle idée de Weil était de reproduire un analogue de la cohomologie singulière, pourtant fortement liée à la topologie réelle, au cadre des variétés sur des corps finis. Ça semble particulièrement surprenant car la géométrie algébrique sur les corps finis semble être un environnement particulièrement hostile à de telles généralisations. La seule topologie « naturelle » dont on puisse munir les variétés est la topologie de Zariski qui est particulièrement grossière. Pour des variétés algébriques il n'est pas possible de dire qu'elles sont « localement isomorphes à une boule », on ne peut pas tracer des lacets ou trianguler la variété, etc, etc. Malgré tous ces obstacles, des mathématiciens sont parvenus à concevoir un cadre formel similaire à celui que l'on obtient avec des variétés munies d'une topologie réelle ou complexe. C'est de cela que je vais vous parler par la suite.

2. Le cadre topologique

2.1. Le groupe fondamental. — L'un des objets fondamentaux de la topologie algébrique est le *groupe fondamental*. Étant donné un espace topologique « sympathique » [1] dont on se fixe un point, on regarde tous les lacets partant de ce point et y revenant. On considère ces objets à déformation continue près et on les munit d'une structure de groupe avec pour loi la concaténation de lacets. Je renvoie à [**4**] pour une définition plus rigoureuse.

Par exemple le plan affine réel a un groupe fondamental trivial, tout lacet partant de l'origine peut être progressivement déformé pour se rétracter sur le point. Considérons maintenant le plan privé d'un point P fixé, il y a alors deux types de lacets : ceux qui « ne font pas le tour de P » et ceux qui « le font ». Les premiers peuvent se rétracter sur un point alors que les autres ne le peuvent pas. On peut prouver que ce plan privé d'un point a un groupe fondamental isomorphe à $\mathbb{Z}$. Via cet isomorphisme la classe d'un lacet est caractérisée par le nombre de fois qu'il fait le

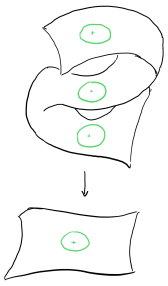
1. Si je reprends le livre de Hatcher [**4**], il faut que l'espace soit connexe, localement connexe par arcs et semi-localement simplement connexe.

tour du point P, le signe étant donné par l'orientation du lacet : fait-il le tour de P dans le sens trigonométrique ou trigonométrique inverse ?

Fort de cette description on peut se demander ce qu'est le groupe fondamental pour nos objets topologiques préférés. Un raisonnement similaire à celui effectué pour le plan, permet de montrer que la sphère $\mathbb{S}^2$ a également un groupe fondamental trivial. Le cercle $\mathbb{S}^1$ a lui un groupe fondamental isomorphe à $\mathbb{Z}$: là encore, la classe d'un lacet est caractérisée par le nombre de fois que l'on a fait le tour du cercle dans un sens ou dans l'autre. Si l'on considère la surface d'un tore de dimension 2 (une bouée) le groupe fondamental est $\mathbb{Z}^2$, caractérisant le nombre de tours suivant des méridiens et le nombre de tours suivant des parallèles. Et puis, si on veut s'amuser un peu on peut étudier des variétés plus baroques comme le plan projectif réel dont le groupe fondamental est de torsion ! C'est $\mathbb{Z}/2\mathbb{Z}$.

La connaissance du groupe fondamental et ses premières propriétés permet de prouver des résultats remarquables tels que le théorème du point fixe de Brouwer en dimension 2 [**4**, Thm. 1.9] : une application continue du disque dans lui-même admet toujours un point fixe. Ou encore le théorème de Borsuk Ulam [**2**, Thm. 20.2] disant que pour toute application continue $\mathbb{S}^2 \to \mathbb{R}^2$ il existe toujours un couple de points antipodaux admettant la même image.

2.2. Les revêtements. — La seconde notion cruciale dans le domaine est celle des revêtements. Un revêtement entre deux espaces topologiques $\pi : X \to Y$ est la donnée d'une application continue surjective que l'on peut *trivialiser localement*. Autrement dit, tout point y de Y admet un voisinage V_y dont l'image réciproque par π est homéomorphe à la réunion disjointe de copies de V_y.



L'image réciproque d'un point est une ensemble discret que l'on appelle sa *fibre* et, s'il est fini, son cardinal ne dépend pas du point, on l'appelle le *degré* du revêtement.

Un revêtement $X \to Y$ induit un morphisme injectif du groupe fondamental de X dans celui de Y. Un espace topologique sympathique X admet un revêtement dit *universel* $\widetilde{X} \to X$ où $\pi_1(\widetilde{X}) = 0$. L'*universalité* vient de ce que tout revêtement de X est un revêtement intermédiaire de $\widetilde{X} \to X$. Autrement dit, pour tout revêtement $Y \to X$ il existe un revêtement $\widetilde{X} \to Y$ rendant le triangle ci-dessous commutatif.

$$\begin{array}{ccc} & & \widetilde{X} \\ & \swarrow & \downarrow \\ Y & \longrightarrow & X \end{array}$$

Par exemple l'application $\mathbb{R} \to \mathbb{S}^1$ définie par $x \mapsto e^{ix}$ réalise est un revêtement universel du cercle.

Plus amusant encore, la théorie des revêtements en topologie algébrique partage de très nombreuses analogies avec la théorie de Galois. Étant donné un revêtement $Y \to X$, le groupe $\pi_1(Y)$ s'identifie à un sous-groupe de $\pi_1(X)$, s'il est distingué, on dit alors que le revêtement est Galoisien. Il y a alors une correspondance entre les sous-groupes de $\pi_1(X)/\pi_1(Y)$ et les revêtements intermédiaires de $Y \to X$. Une autre définition des revêtements Galoisiens, équivalente à la précédente est que le groupe d'automorphisme du revêtement agit librement et transitivement sur la fibre. En particulier, un revêtement fini, *i.e.* de degré fini, est Galoisien si et seulement si son groupe de Galois a un cardinal égal au degré du revêtement.

Selon cette analogie, le revêtement universel jour le rôle de la clôture algébrique (ou séparable) et le groupe fondamental celui du groupe de Galois absolu.

2.3. Homologies et cohomolgies. — Introduisons enfin un troisième ingrédient fondamental en topologie algébrique : les groupes d'homologie, que ce soit l'homologie simpliciale dont la définition est relativement simple à l'homologie singulière, plus lourde mais adaptée à des espaces topologiques bien plus généraux.

Je ne vais pas me lancer ici dans des descriptions détaillées, je me contenterai d'une description informelle. Le groupe fondamental considère des lacets à déformation près. L'homologie va munir les lacets d'une relation d'équivalence plus large que d'être équivalents à déformation près ; deux lacets seront équivalents si leur réunion forme « le bord de quelque chose ». Par exemple dans un tore, deux méridiens seront homologues car forment le bord d'une « coquillette ». Autrement dit, dans le dessin ci-dessous, les deux cercles bleus sont équivalents.

D'une manière générale, l'homologie ou la cohomologie permettent de mesurer des obstructions à rendre globales certaines propriétés locales. Par exemple, sur un tore tout point a un voisinage qui est un disque, un lacet contenu dans ce voisinage sera le bord d'un disque mais cette propriété locale ne se globalise pas : certains lacets tracés sur le tore ne sont pas le bord d'un disque et l'homologie permet de « quantifier » ce défaut.

Enfin, le groupe fondamental π_1 n'est pas sans lien avec la cohomologie, un théorème classique affirme que le premier groupe d'homologie singulière $\mathrm{H}_1(X, \mathbb{Z})$ d'un espace topologique est isomorphe à l'abélianisé de $\pi_1(X)$.

L'homologie singulière permet la démonstration de résultats puissants tels que le *théorème d'invariance du domaine* [**2**, Cor. 19.8] (si un ouvert U de $\mathbb{R}^n$ est homéomorphe à un ouvert V de $\mathbb{R}^m$, alors $n = m$), ou encore le *théorème du point fixe de Brouwer* [**2**, Cor 11.12] (toute application continue de la boule unité de $\mathbb{R}^n$ dans elle même admet un point fixe).

Enfin, l'homologie et la cohomologie singulière sont des constructions fonctorielles : à un espace topologique on associe une collection de groupes (ou de modules) et une application continue entre deux espaces topologiques induit des applications linéaires entre ces modules. Une des utilisations phare de ces applications linéaires est la formule des traces de Lefschetz.

Theorème 2.1 **(Formule des traces de Lefschetz).** — *Soit $f : X \to X$ une application continue d'une variété complexe compacte de dimension d dans elle même, et soit N_f le nombre de points fixes de f comptés avec multiplicité. Alors :*

$$N_f = \sum_{i=0}^{2d} (-1)^i \, Tr(f_i^*)$$

où pour tout i, $f_i^* : H_i(X, \mathbb{Q}) \to H_i(X, \mathbb{Q})$ est l'application linéaire induite par f sur le i-ème groupe d'homologie.

Dans ses travaux, Weil observe un comportement spécifique du nombre de points à coordonnées dans $\mathbb{F}_q$ d'une variété sur un corps fini : il semble provenir d'une formule similaire à la formule des traces de Lefschetz. Il reste « seulement » à construire cette théorie cohomologique. Le contexte impose certaines contraintes. En particulier le corps de définition doit être de caractéristique nulle : on veut le nombre de points et pas seulement le nombre de points modulo la caractéristique. Les

traces dont on va calculer la somme alternée doivent donc vivre dans un corps de caractéristique nulle.

De plus, un exemple dû à Serre considérant certaines courbes elliptiques sur les corps finis, dites *supersingulières* ajoute une nouvelle contrainte : le corps de définition ne peut pas être $\mathbb{Q}, \mathbb{R}$ ou le corps des nombres p-adiques $\mathbb{Q}_p$ où p désigne la caractéristique du corps de définition de la variété algébrique (dont on veut compter les points). Par contre le corps $\mathbb{Q}_\ell$ des nombres ℓ–adiques pour ℓ premier à p reste un candidat possible.

3. Un peu de géométrie algébrique

La tentation est forte : existe-t-il un moyen d'étendre la formule de Lefschetz aux variétés sur un corps finis en prenant pour f le Frobenius ? Cela fournirait une manière de compter les points à coordonnées dans $\mathbb{F}_q$ d'une variété sur ce corps.

Le souci est que dans un monde « continu » on peut tracer des chemins sur une variété. Munie de la topologie usuelle, tout point lisse d'une variété a un voisinage difféomorphe à une boule et enfin, comme on l'a précédemment signalé les revêtements se trivialisent localement. Si on travaille maintenant sur un corps quelconque et (allons-y !) de caractéristique positive, les outils issus de l'analyse et de la topologie usuelle ne sont plus utilisables. On est cantonnés à des outils purement algébriques que je passe rapidement en revue dans ce qui suit.

3.1. Variétés, fonctions. — Je ne vais pas ici faire un cours détaillé de géométrie algébrique, simplement dire que son but est d'étudier de manière géométrique le lieu d'annulation d'un ensemble de polynômes. Plus important encore que l'objet géométrique lui-même, il y a les fonctions que l'on définit dessus. En géométrie algébrique, les fonctions « autorisées » sont les polynômes et/ou les fractions rationnelles : les fonctions algébriques. Le fameux théorème des zéros de Hilbert (*Nullstellensatz*) établit une correspondance entre sous-ensembles algébriques d'un ensemble algébrique et idéaux de l'anneau des fonctions définies sur la variété. On munit alors naturellement une variété d'une topologie, la *topologie de Zariski* : les fermés sont les lieux d'annulation d'un polynôme.

Cette topologie est particulièrement grossière. Par exemple les fermés d'une courbe sont ; la courbe elle-même et ses sous-ensembles finis. En particulier les espaces topologiques ainsi obtenus ne sont pas séparés [2]. Pire que ça : tout ouvert est dense.

3.2. Études locales. — Comme en géométrie différentielle, on sait étudier une fonction ou une variété *au voisinage d'un point* donné. On dispose en particulier en chaque point d'une variété, d'un anneau local des fonctions algébriques définies au voisinage de ce point : l'ensemble des fractions rationnelles dont le dénominateur ne s'annule pas en ce point. Ces anneaux locaux sont fort pratiques mais restent en un sens décevants : étant donnés deux points non singuliers d'une variété algébrique, les anneaux locaux ne sont en général pas isomorphes. Même en considérant les anneaux locaux, on ne parvient donc pas à retrouver cette description plaisante des variétés topologiques comme un ensemble pour lequel les voisinages de deux points distincts sont homéomorphes. Une remarque toutefois qui prendra son sens plus tard : si les anneaux locaux au voisinage de 2 points distincts ne sont pas isomorphes, leurs complétés [3] le sont.

Puisqu'on parlait de revêtements dans la section précédente, on peut définir des morphismes de variétés algébriques. Certains, comme les revêtements, vérifient la propriété qu'une fibre a toujours le même cardinal. On parle alors de *revêtement non ramifié* ou *revêtement étale.* [4]

2. En géométrie algébrique, une notion de *séparation* existe mais elle est plus faible que la définition usuelle en topologie

3. Je renvoie à [**3**, Chap. 7] pour la notion de complétion d'anneau local.

4. La terminologie n'est pas complètement cohérente entre topologie algébrique et géométrie algébrique. En topologie, un *revêtement ramifié* est une application continue qui devient un revêtement si l'on supprime certains points. Ensuite, toujours en topologie, quand on parle de *revêtement* (tout court) il est non ramifié. En géométrie algébrique, lorsque l'on parle de *revêtement*, il est possiblement ramifié et, s'il ne l'est pas, on le précise en parlant de revêtement *non ramifié* ou *étale*.

On peut associer aux revêtements un groupe d'automorphismes et certains morphismes s'avèrent être des revêtements *Galoisiens* : le groupe d'automorphismes agit librement transitivement sur toute fibre. Un théorème de correspondance de Galois existe et établit une correspondance entre sous-groupes du groupe d'automorphismes d'un morphisme et revêtements intermédiaires. Par ailleurs on dispose d'un foncteur contravariant entre variétés et corps de fonctions algébriques (*i.e.* extensions finies du corps de fonctions rationnelles $k(x_1, \ldots, x_n)$) et via ce foncteur, le théorème de correspondance de Galois pour les morphismes entre variétés correspond au théorème de correspondance de Galois bien connu pour les extensions de corps.

Mais pour autant, le caractère trop grossier de la topologie de Zariski ne permet pas de trivialiser localement un revêtement entre variétés : il n'y a pas assez d'ouverts et ils sont bien « trop gros ».

3.3. Faisceaux. — Bon... faut bien que j'en parle à un moment, une des premières marches un peu pénible à franchir en géométrie algébrique, ce sont les faisceaux. Conceptuellement, ce n'est pas si lourd : au lycée quand vous parliez de fonction, votre prof commençait par vous dire « quel est le domaine de définition ? ». Un faisceau sur un espace topologique X, c'est une collection de couples (U, f) où U est un ouvert de X, f est une fonction définie sur U, à laquelle on rajoute deux propriétés :

— Une stabilité par restriction : si V est contenu dans U alors la je peux définir une restriction $f_{|V}$ de f à V et le couple $(V, f_{|V})$ fait partie du faisceau ;
— Une stabilité par « recollement », si (U, f) et (U', g) sont coïncident $U \cap U'$ (autrement dit les restrictions sont égales) alors il existe un unique « recollement » défini sur $U \cup U'$.

Plus formellement, l'ensemble des ouverts de X ordonnés par inclusion forme une catégorie dont les flèches sont données par les inclusions. Un faisceau d'ensembles est un foncteur contravariant de cette catégorie des ouverts vers la catégorie des ensembles vérifiant une certaine propriété de recollement. En résumé : à un ouvert U, on associe un ensemble $F(U)$ de fonctions sur cet ouvert, la fonctorialité n'est autre que la stabilité par restriction. Ensuite, il faut ajouter une propriété de recollement. Pour finir, on peut spécifier la catégorie d'arrivée pour avoir des faisceaux en groupes, en anneaux, etc.

Remarque 3.1. — *Assumant un style très discursif et parfois obscur (je m'adapte à l'environnement sous-terrain), je vais parfois loin dans le manque de rigueur. Sur les faisceaux, la définition rigoureuse ne demande pas que f soit une fonction sur U, c'est un objet d'une certaine catégorie. Cependant, un théorème que je ne détaille pas affirme que tout faisceau est isomorphe à un faisceau de fonctions à valeurs dans un ensemble* ad hoc *appelé* espace étalé du faisceau.

Des faisceaux vous en connaissez plein. Sur la droite réelle, il y a le faisceau des fonctions continues, des fonctions $\mathcal{C}^\infty$. Sur $\mathbb{C}$, il y a le faisceau des fonctions holomorphes, etc. etc.

Un aspect sympathique des faisceaux est qu'ils s'accompagnent d'une cohomologie du même nom : la cohomologie des faisceaux. Suivant le bon vieux principe de « pourquoi faire simple quand on peut faire compliqué », la cohomologie simpliciale, relativement simple à définir peut quand même se voir comme la cohomologie d'un faisceau constant : autrement dit la cohomologie d'un faisceau de fonctions localement constantes à valeurs entières. Mais cette dernière observation nécessite une fois de plus que l'on munisse l'objet d'étude d'une topologie de variété topologique réelle et donc que l'on dispose de « beaucoup d'ouverts ». Appliqué à la topologie de Zariski, on fait de nouveau face à un échec cuisant : appliqué à une variété algébrique connexe munie de la topologie de Zariski, le faisceau constant $\mathbb{Z}$, autrement dit le faisceau des fonctions localement constantes (donc constantes parce que tout ouvert est dense) à valeurs entières donne un H^0 de dimension 1 (une seule composante connexe) et des H^i nuls pour tout $i > 0$.

4. Topologie et cohomologie étale

4.1. On veut faire quoi déjà ? — Si on fait le bilan de la discussion précédente, on veut trouver une cohomologie dans l'esprit de la cohomologie singulière/simpliciale que l'on puisse décrire de manière purement algébrique. On semble bloqué à plusieurs endroits :

— On ne peut pas trivialiser localement une variété, autrement dit on ne peut pas dire que dans une variété, deux points lisses ont des voisinages homéomorphes ;
— On peut définir des revêtements et une théorie de Galois de ces derniers, mais on ne peut pas les trivialiser localement ;
— Les faisceaux constants ont une cohomologie sans intérêt.

Et ces constats reposent sur un même problème : la topologie de Zariski, pourtant naturelle en géométrie algébrique, n'est pas adaptée parce que beaucoup trop grossière.

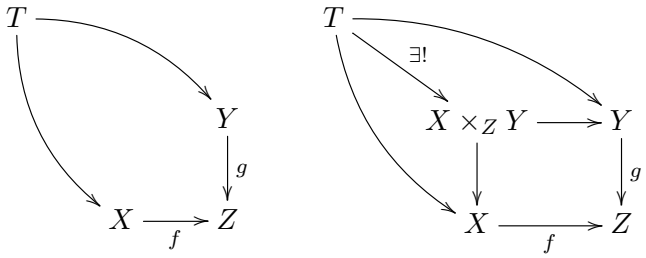
4.2. Eurêka. — L'idée clé et absolument géniale introduite par Grothendieck est de dire que le problème n'est pas dans « Zariski » mais dans « topologie ». Il propose alors de relaxer la définition de topologie en supprimant une propriété (pourtant assez intuitive) : dans une *topologie de Grothendieck* sur une variété algébrique, un ouvert n'a pas besoin d'être un sous-ensemble de cette variété...

Si on reprend la définition d'une topologie, c'est un ensemble de parties d'un ensemble X incluant la partie vide $\emptyset$, la partie pleine X et stable par unions quelconques et par intersections finies. Comme je l'avais mentionné précédemment, une topologie a une structure naturelle de catégorie, les morphismes étant donnés par les relations d'inclusion. Une topologie de Grothendieck, se définit ainsi comme une catégorie d'« ouverts » munies des quelques propriétés strictement nécessaires pour pouvoir y étendre la notion de faisceau. À savoir :

— il faut généraliser la notion d'intersection qui sera remplacée par le fait que la catégorie soit stable par produit fibré. Je reviens sur ce point un peu après.
— il faut généraliser la notion de recouvrement par des ouverts (pas besoin de généraliser exactement la stabilité par union quelconque : la cible c'est de pouvoir définir des faisceaux dans ce contexte), ce qui est fait par une propriété adéquate.

Un faisceau, devient alors un foncteur de la topologie de Grothendieck (qui est une catégorie) à valeurs dans une autre catégorie (celle des groupes abéliens par exemple) vérifiant une propriété de recollement impliquant les recouvrements d'ouverts apparaissant dans la définition de topologie de Grothendieck.

Pourquoi le produit fibré ? — Dans une catégorie si on se donne trois objets X, Y, Z et des flèches $f : x \to Z$ et $g : Y \to Z$, le produit fibré $X \times_Z Y$ est (s'il existe), un objet vérifiant la propriété universelle suivante : tout diagramme commutatif comme celui de gauche dans la figure se factorise de manière unique en le diagramme commutatif de droite :



Si par exemple on est dans la catégorie des ensembles le produit fibré existe et a une description explicite simple :

$$X \times_Z Y \overset{\text{def}}{=} \{(x, y) \in X \times Y \mid f(x) = g(y)\}.$$

Si maintenant, X, Y sont inclus dans Z et que les applications f, g sont les injections canoniques, on déduit alors que le produit fibré n'est autre que l'intersection $X \cap Y$. Aussi, la propriété de stabilité par produits fibrés dans les catégories de Grothendieck est une généralisation naturelle de la propriété de stabilité par intersections finies des topologies au sens classique.

4.3. Les ouverts, c'est comme la confiture, moins on en a, plus on l'étale. — Reste l'épineuse question de « quelle topologie de Grothendieck » ? La topologie étale consiste en les ouverts de Zariski mais également leurs revêtements étales. Si par exemple on considère la droite affine $\mathbb{A}^1$ et l'ouvert de Zariski $\mathcal{U} \overset{\text{def}}{=} \mathbb{A}^1 \setminus \{0\}$ est un ouvert pour la topologie étale. Mais le

revêtement non ramifié

$$\begin{cases} \mathcal{U} & \longmapsto & \mathcal{U} \\ z & \longrightarrow & z^2. \end{cases}$$

en est un autre. Voici un autre exemple, toujours d'ouvert étale de $\mathbb{A}^1$. On considère la courbe affine $\mathcal{E}$ plane d'équation $y^2 = x(x+1)(x-1)$ et P, Q, R les points de coordonnées respectives $(-1,0), (0,0), (1,0)$. Alors, le revêtement

$$\begin{cases} \mathcal{E} \setminus \{P,Q,R\} & \longmapsto & \mathbb{A}^1 \setminus \{-1,0,1\} \\ (x,y) & \longrightarrow & x. \end{cases}$$

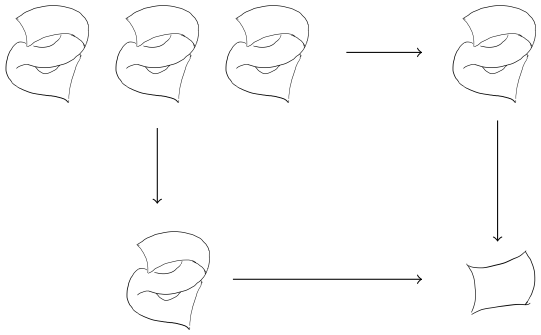
est un revêtement non ramifié de $\mathbb{A}^1 \setminus \{-1,0,1\}$, et donc un ouvert étale de $\mathbb{A}^1$!

4.4. Et ça apporte quoi ? — Ben, ça résout plein de problèmes ! On n'arrivera toujours pas à dire que deux points d'une variété ont des voisinages ouverts isomorphes mais au moins les anneaux locaux deviennent isomorphes. En effet, l'anneau local pour la topologie étale correspond à la partie algébrique du complété de l'anneau local pour la topologie de Zariski et comme je l'avais mentionné avant cela, si les anneaux locaux pour la topologie de Zariski ne sont pas isomorphes, leurs complétés le sont.

Ensuite, il y a suffisamment d'ouverts pour trivialiser des revêtements non ramifiés et la trivialisation locale d'un revêtement se fait presque... *par construction*. Si on se donne une variété X et un revêtement non ramifié $Y \to X$. Alors ce revêtement est aussi... un ouvert pour la topologie étale, on peut donc restreindre le revêtement à cet ouvert ! Revenons au cas d'un revêtement topologique classique $p : Y \to X$. On se donne un point de X, la trivialisation locale consiste à dire qu'il existe un voisinage ouvert $\mathcal{U}$ de X tel que $p^{-1}(U)$ est homéomorphe à une réunion disjointe de copies de $\mathcal{U}$. Cela peut se reformuler en disant que le produit fibré $\mathcal{U} \times_X Y$ (pour l'injection canonique $\mathcal{U} \hookrightarrow X$ et $p : Y \to X$) est homéomorphe à une union disjointes de copies de $\mathcal{U}$.

Si l'on revient maintenant à un revêtement étale $Y \to X$, alors, dans les diagrammes ci-dessous, en regardant $Y \to X$ à la verticale comme un revêtement et à l'horizontale comme un ouvert pour notre topologie (de Grothendieck) étale, on peut prouver que le produit fibré $Y \times_X Y$ nous donne... une réunion disjointe de copies de Y ! Autrement dit, le revêtement se trivialise au voisinage de chaque point en considérant le même voisinage pour chaque point qui ne sera rien d'autre que le revêtement lui même.

$$\begin{array}{ccc} Y \times_X Y & \longrightarrow & Y \\ \downarrow & & \downarrow \\ Y & \longrightarrow & X \end{array}$$



Fort de ce constat, on revient au groupe fondamental. Sa définition classique repose sur le tracé et la déformation de lacets sur un espace topologique. Mais la théorie des revêtements le faisait aussi apparaître comme une sorte de groupe de Galois. Un groupe qui permet de classifier les revêtements d'un espace topologique donné. Ce point de vue s'étend bien plus facilement au cadre algébrique. On définit ainsi le groupe fondamental d'une variété comme la limite projective des groupes d'automorphismes de tous ses revêtements étales Galoisiens. Autrement dit, un gros groupe dont les quotients finis sont les groupes de Galois de revêtements étales finis. Pour une variété complexe, le groupe ainsi obtenu est le complété, pour une certaine topologie, du groupe fondamental « classique » défini dans le cas topologique. Pour finir, même s'il faut sortir de la catégorie des ouverts de Zariski et aller chercher des ouverts étales pour trivialiser un revêtement, notre définition du $\pi_1(X)$ conserve une propriété vérifiée dans le cadre topologique : il agit transitivement sur la fibre de tout revêtement de X.

4.5. L'apothéose. — Enfin, la cohomologie des faisceaux constants qui était triviale pour la topologie de Zariski devient non triviale et fournit un outil d'une grande richesse qui mènera à la preuve des conjectures de Weil. Si on considère une variété X sur un corps fini munie du faisceau constant μ_ℓ (c'est-à-dire, le faisceau des fonctions localement constantes à valeurs dans le groupe des racines ℓ-ièmes de l'unité) où ℓ est premier à la caractéristique, on peut considérer la suite exacte de Kummer :

$$0 \longrightarrow \mu_\ell \longrightarrow \mathcal{O}^\times \xrightarrow{f \mapsto f^\ell} \mathcal{O}^\times \longrightarrow 0,$$

où $\mathcal{O}^\times$ décrit le faisceau des fonctions algébriques (autrement dit les polynômes et les fractions rationnelles) sur X sans zéros ni pôle sur leur ouvert de définition. Ces faisceaux peuvent être définis pour la topologie de Zariski mais cette suite ne serait pas exacte à droite : en effet l'application $f \mapsto f^\ell$ définit un morphisme de faisceaux mais celui-ci n'est pas surjectif : si on travaille par exemple sur un ouvert de la droite affine $\mathbb{A}^1$, une fraction rationnelle f ne peut pas s'écrire comme une puissance ℓ-ième, même si on se restreint à un sous-ouvert. Dans le cadre étale, cela devient possible en considérant un revêtement étale d'un ouvert de la droite du type $Y \to \mathbb{A}^1$ où Y serait un ouvert de la courbe d'équation $T^\ell - f(X) = 0$. Sur Y la fonction f devient une puissance ℓ-ième. La topologie étale permet donc de rendre exactes des suites de faisceaux qui ne le seraient pas avec la seule topologie de Zariski.

La suite exacte de Kummer permet de déduire le $\mathrm{H}^1_{\text{ét}}(X, \mu_\ell)$ de la connaissance de $\mathrm{H}^1_{\text{ét}}(X, \mathcal{O}^\times)$. On prouve que ce dernier n'est autre que le groupe de Picard de la courbe (un analogue géométrique du groupe de classes en théorie des nombres). En transpirant un peu, on en déduit que ce $\mathrm{H}^1_{\text{ét}}(X, \mu_\ell)$ est isomorphe à la ℓ–torsion du groupe de Picard de X et classifie les revêtements étales Galoisiens de degré ℓ de la variété. Plus formellement, $\mathrm{H}^1_{\text{ét}}(X, \mu_\ell)$ est isomorphe à $\mathrm{Hom}(\pi_1(X), \mathbb{Z}/\ell\mathbb{Z})$ une relation proche de celle obtenue dans le cadre topologique (le H_1 égal à l'abélianisé du π_1) ! Si de plus X est une courbe de genre g, on prouve que ce $\mathrm{H}^1_{\text{ét}}$ est de dimension $2g$, ce qui est également la dimension des H^1 de la cohomologie singulière ou simpliciale d'une courbe complexe. On tient le bon bout ! Le groupe de cohomologie $\mathrm{H}^1_{\text{ét}}(X, \mathbb{Q}_\ell)$ se déduit des groupes de type $\mathrm{H}^1_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$ par la construction :

$$\mathrm{H}^1_{\text{ét}}(X, \mathbb{Q}_\ell) = \left(\varprojlim \mathrm{H}^1_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Deligne a prouvé que cette construction répondait à toutes les attentes les plus folles énoncées par Weil. Autrement dit, c'est une cohomologie de Weil, en particulier elle fournit une formule des traces de Lefschetz et l'endomorphisme de Frobenius sur X induit des endomorphismes sur les groupes de cohomologie auxquels on peut appliquer cette formule des traces et déduire une formule sur le nombre de points rationnels de X. En définitive, la construction de la cohomologie étale fournit exactement l'outil dont on rêvait.

5. Retours à nos moutons

Découvrir cette théorie m'a enchanté, même si je n'aurais pas la prétention de dire que j'en connais les moindres détails. La cohomologie étale a permis de résoudre une conjecture majeure en géométrie arithmétique pour autant elle ne m'a pas aidé à remplir mes objectifs initiaux : l'utiliser pour résoudre des problèmes relatifs aux codes correcteurs d'erreurs. Dès que l'on ne travaille plus sur une courbe les groupes de cohomologie et l'action du Frobenius sur ces derniers devient très difficile à calculer en pratique. D'ailleurs, cela ne fait qu'une dizaine d'années que l'on sait que ces objets sont calculables (au sens de Church–Turing) [**7**]. Pour les courbes, la borne de Weil sur le nombre de points

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leqslant 2g\sqrt{q}$$

peut se déduire de la preuve des conjectures de Weil.... mais elle peut s'obtenir via des constructions plus simples. Par ailleurs, cette borne s'avère être précise pour de grandes valeurs de q alors que la théorie des codes est friande de constructions sur de petits corps finis. Et sur de petits corps, les méthodes de comptage reposant sur de la combinatoire et de la géométrie finie sont parfois plus efficaces que les formules utilisant la cohomologie étale. Bref, je ne suis pas parvenu

à l'utiliser à bon escient pour obtenir des propriétés de codes. Mais ce n'est que partie remise et cela n'enlève rien à la beauté de la construction.

Bon... il est temps de remonter à la surface (qui n'est même pas algébrique).

Remerciements

Un grand merci aux organisateurs de Ktorphée et aux participants (A., B., L., M., P. et Q.) de cette sortie pour cette formidable nuit d'escapade spéléo-mathématique ! Sincère remerciements à Christophe Levrat qui n'écoutant que son courage m'a sauvé d'une terrible noyade dans des algèbres centrales simples.

Références

[1] Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Inform. Theory **24** (1978), no. 3, 384–386.

[2] Glen E. Bredon, *Topology and geometry*, Graduate Texts in Mathematics, no. vol. 14, Springer, 1993.

[3] David Eisenbud, *Commutative algebra : With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer, 1995.

[4] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.

[5] Gilles Lachaud, *Projective Reed-Muller codes*, Coding theory and applications (Cachan, 1986), Lecture Notes in Comput. Sci., vol. 311, Springer, Berlin, 1988, pp. 125–129. MR MR960714 (89i :94038)

[6] John B. Little, *Algebraic geometry codes from higher dimensional varieties*, Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 257–293.

[7] David A. Madore and Fabrice Orgogozo, *Calculabilité de la cohomologie étale modulo ℓ*, Algebra and Number Theory **9** (2015), no. 7, 1647–1739 (Français).

[8] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[9] ———, *Lectures on Étale Cohomology (v2.21)*, 2013, Available at `www.jmilne.org/math/`, p. 202.

[10] Judy L. Walker, *Codes and curves*, AMS, Student Mathematical Library, IAS/Park City, 2000, `https://cdn.preterhuman.net/texts/math/Codes%20and%20Curves.pdf`.

A. C., Quelque part sous Paris, en direction du Nord