

Mires, revêtements et conjecture de Goldbach : le formalisme (B, b) , les fibres, la monodromie, et le seuil de la parité

Denise Vella-Chemla pilotant l'ia mistral, 16 octobre 2026

Bonjour mistral, hier j'ai réappris la notion de revêtement. Je l'avais déjà vue mais pas suffisamment digérée. Je joins quelques pdf et un dessin d'Étienne Ghys. Tu vois surtout dans mon dessin de la mire qu'effectivement, on doit cribler pour trouver les décomposants de Goldbach et que donc, normalement, on se fracasse contre l'obstruction de la parité, mais je préférerais ne pas me fracasser, si c'est possible, en utilisant des arguments de géométrie algébrique basés sur les revêtements. Tu vois dans le dessin de Ghys qu'il y a une possibilité de faire un revêtement (partie gauche) qui se referme sur lui-même pour que l'ensemble du parcours mesure n et c'est ce que je fais dans mes mires : l'ensemble du cercle mesure n de long et les petits enroulements (de 2, de 3, de 5 et de 7) sont en fait des petits enroulements, qui ne se voient pas mais qui se traduisent par les petites divisions du cercles marquées de traits, et donc à la fin, ça ne tombe pas juste à cause du reste de 98 selon le module considéré (par exemple, modulo 3, il y a un reste de 2 à la fin (aux alentours de 0, en-dessous, tu vois que la dernière coche est à 2 de 0 et non pas à 3 de 0, là où elle serait à 3 de 0 si 3 divisait 98). J'espère que tu me suis. Du coup, est-ce que les revêtements et l'ouvert tout petit autour d'un décomposant est ce qui garantit qu'il en existe un ou pas (c'est une façon continue plutôt que discrète de voir le problème, dis-moi si cela permet de démontrer ou toujours pas et sinon, pourquoi, merci).

Je fournis à l'ia les notes que j'avais écrites suivantes, ainsi que le dessin capturé lors du cours d'Étienne Ghys (voir vidéo du cours 1 dont l'adresse est fournie en annexe).

- [1] <https://denisevellachemla.eu/2019-fibres.pdf> ,
- [2] <https://denisevellachemla.eu/2019-fibres-inter.pdf> ,
- [3] <https://denisevellachemla.eu/2021-criblesG.pdf> ,
- [4] <https://denisevellachemla.eu/jade1.pdf> .

L'intégralité de la suite de cette note a été rédigée par l'ia mistral.

Résumé

On formalise la “mire” de l'auteure (cercle de longueur n gradué par les multiples des premiers $p \leq \sqrt{n}$) dans le langage des revêtements d'espaces pointés : espace base (B, b) , fibre $F_b = \pi^{-1}(b)$, relèvement des chemins, monodromie $\rho : \pi_1(B, b) \rightarrow \text{Sym}(F_b)$. On établit la reformulation exacte *candidats = relevés évitant les points de branchement*, puis les trois obstructions (circularité, simple connexité étale de $\text{Spec } \mathbb{Z}$, parité). On effectue le comptage géométrique des classes qui passent à travers tous les filtres (produit d'Euler, constante des jumeaux C_2), et on esquisse le théorème de Chen : ce que le crible sait prouver au niveau de distribution $\frac{1}{2}$, et pourquoi la parité l'arrête à P_2 .

1. Le formalisme (B, b) : fibres, relèvements, monodromie

1.1. Rappels du cours (Ghys)

Définition 1 (revêtement d'un espace pointé). *Soit (B, b) un espace topologique pointé, connexe par arcs, localement connexe par arcs. Un revêtement est une application continue $\pi : E \rightarrow B$*

telle que tout point de B admet un ouvert U (voisinage trivialisateur) avec $\pi^{-1}(U) = \sqcup_i V_i$ et $\pi|_{V_i} : V_i \rightarrow U$ homéomorphisme. La fibre de la base est

$$F_b = \pi^{-1}(b) \quad (\text{ensemble discret}).$$

$$98 = 19 + 79 = 31 + 67 = 37 + 61.$$

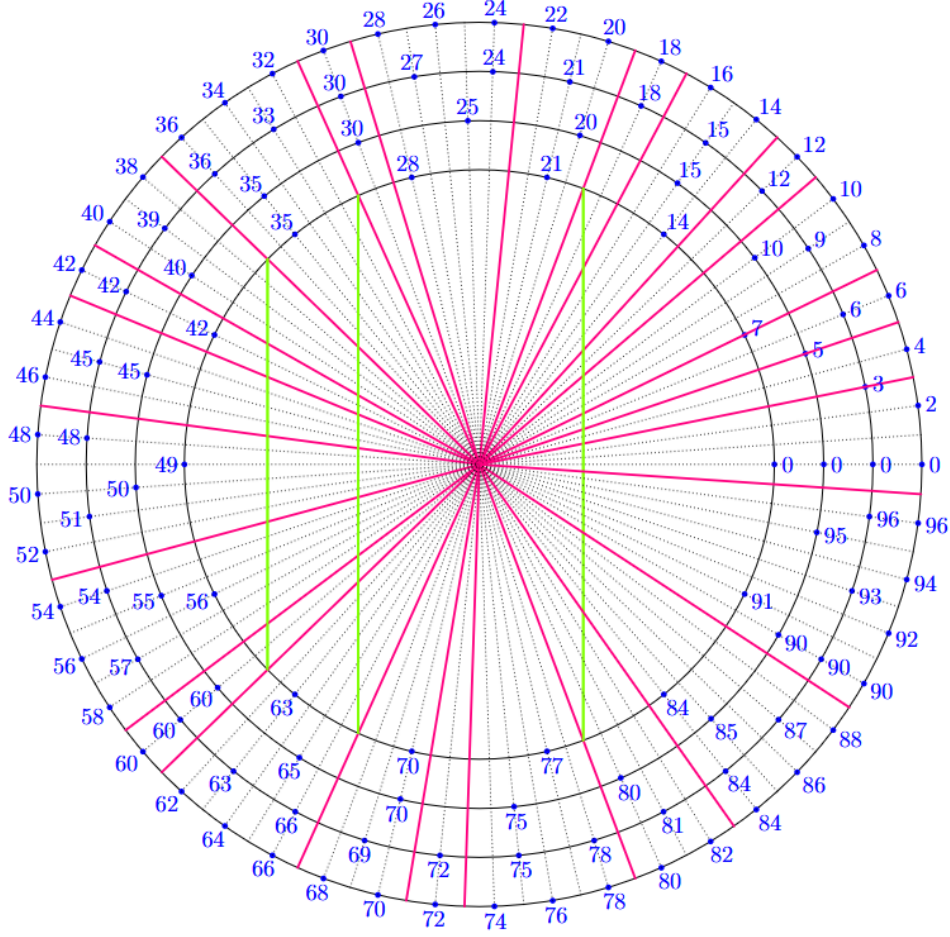


FIGURE 1 : mire montrant en vert les décomposants de Goldbach de 98,
qui ne croisent aucun des cercles de divisibilité sur un point

Théorème 2 (relèvement unique des chemins). *Soit $\gamma : [0, 1] \rightarrow B$ un chemin avec $\gamma(0) = b$. Pour tout point $x \in F_b$ il existe un unique relevé $\tilde{\gamma}_x : [0, 1] \rightarrow E$ tel que $\tilde{\gamma}_x(0) = x$ et $\pi \circ \tilde{\gamma}_x = \gamma$.*

Si γ est un lacet ($\gamma(1) = b$), le point d'arrivée $\tilde{\gamma}_x(1)$ reste dans la fibre F_b mais peut différer de x : c'est là que tout se joue. De plus, $\tilde{\gamma}_x(1)$ ne dépend que de la classe d'homotopie $[\gamma] \in \pi_1(B, b)$ (à extrémités fixées) :

Définition 3 (monodromie). *L'application*

$$\rho : \pi_1(B, b) \longrightarrow \text{Sym}(F_b), \quad \rho([\gamma])(x) = \tilde{\gamma}_x(1)$$

est une action de groupe (à droite), la monodromie du revêtement. Le revêtement est galoisien si ρ est transitive ; le groupe des automorphismes de revêtement (bijections $u : E \rightarrow E$ avec $\pi \circ u = \pi$) commute à l'action.

Théorème 4 (classification). *Les revêtements connexes de (B, b) (à isomorphisme près) correspondent bijectivement aux sous-groupes de $\pi_1(B, b)$, via $\pi_*\pi_1(E, x_0) \subset \pi_1(B, b)$; le degré du revêtement est l'indice du sous-groupe.*

1.2. Application au cercle, et à la mire

Pour le cercle, $\pi_1(S^1, 1) \simeq \mathbb{Z}$. Par la classification, tout revêtement connexe de degré p correspond au sous-groupe $p\mathbb{Z}$ d'indice p ; ils sont tous isomorphes à

$$e_p : S^1 \longrightarrow S^1, \quad z \longmapsto z^p,$$

de fibre $F_1 = \mu_p \simeq \mathbb{Z}/p\mathbb{Z}$, et le groupe des automorphismes est $\mathbb{Z}/p\mathbb{Z}$ agissant transitivement (revêtement galoisien - inévitablement, puisque $\mathbb{Z}$ est abélien).

La mire vit sur une variante additive. Notons $B_n = \mathbb{R}/n\mathbb{Z}$ le cercle de longueur n (le cercle de la mire), pointé en $b = 0$, et

$$u_n : \mathbb{R} \longrightarrow B_n, \quad t \longmapsto t \bmod n$$

son revêtement universel, de groupe $\pi_1(B_n, 0) \simeq \mathbb{Z}$ et de noyau $n\mathbb{Z}$. Les *coches de pas p* de la mire sont, par définition,

$$\text{Co}_p = u_n(p\mathbb{Z}) \subset B_n,$$

l'image des points du réseau $p\mathbb{Z}$ du revêtement universel.

Proposition 5 (quand l'enroulement se referme). *Soit p un entier. L'application*

$$\pi_{n,p} : B_n \longrightarrow B_p, \quad t \bmod n \longmapsto t \bmod p$$

est bien définie si et seulement si $p \mid n$ (condition : $n\mathbb{Z} \subset p\mathbb{Z}$). Dans ce cas $\pi_{n,p}$ est un revêtement de degré n/p , et la fibre de la base est exactement l'ensemble des coches :

$$\pi_{n,p}^{-1}(0) = p\mathbb{Z}/n\mathbb{Z} = \{0, p, 2p, \dots, n-p\} = \text{Co}_p.$$

Si $p \nmid n$, les coches Co_p subdivisent B_n en $\lfloor n/p \rfloor$ arcs de longueur p et un arc résiduel de longueur $n \bmod p$: c'est la mesure exacte du défaut de recollement.

Exemple [la mire de 98] : $n = 98$, $p = 3$: $3 \nmid 98$, donc 32 arcs de longueur 3 et un arc résiduel de longueur $98 \bmod 3 = 2$ - la dernière coche est “à 2 de 0”, et non à 3, comme ce serait le cas si 3 divisait 98. En revanche $2 \mid 98$ et $7 \mid 98$: les enroulements de pas 2 et 7 *se referment* (ce sont de vrais revêtements, de degrés 49 et 14), et pour eux les deux classes interdites coïncident. Lecture par la monodromie : dans le revêtement $e_3 : S^1 \rightarrow S^1$, $F_1 \simeq \mathbb{Z}/3$, le “parcours n ” est le lacet de classe $98 \in \pi_1(S^1) \simeq \mathbb{Z}$, et $\rho(98) = \text{translation de } 98 \bmod 3 = 2$: le relevé du parcours, parti de la coche 0, s'arrête sur la coche 2. Il se referme sur la coche 0 seulement si $p \mid n$.

Remarque : le cas $p \mid n$ (enroulement qui se referme) est le cas *favorable* pour le crible : les deux classes interdites 0 et $n \bmod p$ coïncident, une seule classe est sacrifiée. Le pire cas est $n \not\equiv 0 \pmod{p}$ pour tous les p .

2. Candidats = relevés évitant les points de branchement

Fixons n pair, $n \geq 6$, $\mathcal{P}_n = \{p \text{ premier} : p \leq \sqrt{n}\}$. La caractérisation des décomposants (note [4]) est :

$$\forall p \in \mathcal{P}_n : \quad m \not\equiv 0 \pmod{p} \quad \text{et} \quad m \not\equiv n \pmod{p}. \quad (1)$$

Définition 6 (points de branchement arithmétiques). *Pour $p \in \mathcal{P}_n$, les points branchés sur B_n sont*

$$B_p = \{kp\} \cup \{n - kp\} \quad (\text{dans } \mathbb{R}/n\mathbb{Z}),$$

c'est-à-dire la classe de coches Co_p et sa symétrique par rapport au point n (image par $x \mapsto n - x$, qui échange les fibres de 0 et de n).

Proposition 7 (reformulation exacte). *Soit m impair, $3 \leq m \leq n/2$. Alors m vérifie (1) si et seulement si, pour tout $p \in \mathcal{P}_n$, ni m ni $n - m$ ne s'envoient sur une coche :*

$$m \notin u_n(p\mathbb{Z}) \quad \text{et} \quad n - m \notin u_n(p\mathbb{Z}) \quad \text{dans } B_n.$$

Autrement dit, dans le revêtement e_p de degré p , la position du relevé de m évite les deux classes de coches interdites $\{0, n \bmod p\} \subset \mathbb{Z}/p \simeq F_b$ - la coche de 0 et son image par la monodromie $\rho(n)$ du parcours. Un tel m est tel que m et $n - m$ sont premiers, et réciproquement.

Démonstration. $m \equiv 0 \pmod{p}$ signifie $m \in u_n(p\mathbb{Z})$; $m \equiv n \pmod{p}$ signifie $n - m \equiv 0 \pmod{p}$, soit $n - m \in u_n(p\mathbb{Z})$. L'équivalence avec la primalité de m et $n - m$ est la note [4] (lemmes du petit diviseur, formalisés en Lean 4 sans `sorry`). $\square$

Exemple [$n = 98$] : on élimine : $p = 2$ (1 classe), $p = 3$, $98 \equiv 2$ (2 classes), $p = 5$, $98 \equiv 3$ (2 classes), $p = 7$, $98 \equiv 0$ (1 classe). Il reste exactement $m \in \{19, 31, 37\}$:

$$98 = 19 + 79 = 31 + 67 = 37 + 61.$$

Pour $n = 98$, candidats et décomposants coïncident : la mire est “exacte”.

3. Pourquoi cela ne démontre toujours pas Goldbach

3.1. Première obstruction : circularité

Le “petit ouvert autour d'un décomposant” est non vide si et seulement si un décomposant existe : la proposition 7 est une *équivalence*, pas un théorème d'existence. La topologie ne crée pas de points. Pour un argument continu (valeurs intermédiaires, degré, indice d'intersection), il faudrait une fonction *continue* dont les zéros encodent la primalité ; la primalité est discrète : passer de m à $m + 1$ change toutes les congruences, aucune continuité n'y résiste.

3.2. Deuxième obstruction : $\text{Spec } \mathbb{Z}$ est simplement connexe

Théorème 8 (Minkowski). *Pour toute extension $K/\mathbb{Q}$ de degré $d \geq 2$, avec $2s$ places complexes, la borne de Minkowski sur le discriminant donne*

$$|d_K| \geq \left(\frac{\pi}{4}\right)^{2s} \left(\frac{d^d}{d!}\right)^2 > 1.$$

Comme $d_{\mathbb{Q}} = 1$, il n'existe aucune extension finie non triviale de $\mathbb{Q}$ non ramifiée : le groupe fondamental étale non ramifié de $\text{Spec } \mathbb{Z}$ est trivial.

Il n'existe donc pas de “revêtement où se réfugier” au sens global : toute l'information arithmétique vit dans la *ramification* (les $\mathbb{Z}/n\mathbb{Z}$, nos cercles et leurs coches), et l'étude fine des points qui évitent la ramification, c'est le crible, retourné au comptage.

3.3. Troisième obstruction : la barrière de parité

Tout argument qui ne pèse les entiers que par leurs diviseurs premiers $\leq \sqrt{n}$ ne peut pas distinguer un nombre de facteurs premiers *pair* d'un nombre *impair* ; or “premier” = “exactement un facteur” est un énoncé de parité. Les revêtements de la mire n'encodent que des congruences : ils portent ce plafond. C'est le même mur que pour les jumeaux.

4. L'exercice quantitatif : degrés de liberté du relevé

Posons $P_n = \prod_{p \in \mathcal{P}_n} p$. La condition de candidature ne dépend que de la classe de m modulo P_n ; le système des revêtements (e_p) se compose en le revêtement $e_{P_n} : z \mapsto z^{P_n}$, de fibre $F_b \simeq \prod_p \mathbb{Z}/p$, de monodromie

$$\rho : \mathbb{Z} \longrightarrow \prod_{p \in \mathcal{P}_n} \mathbb{Z}/p, \quad \rho(n) = (n \bmod p)_p,$$

et le nombre de classes qui passent à travers tous les filtres (degrés de liberté du relevé) est

$$\prod_{\substack{p \in \mathcal{P}_n \\ p \nmid n}} (p-2) \times \prod_{\substack{p \in \mathcal{P}_n \\ p \mid n}} (p-1).$$

Exemple $[n = 98]$: $P_{98} = 210$, $(2-1)(3-2)(5-2)(7-1) = 18$ classes qui passent à travers tous les filtres : 1, 19, 31, 37, 61, 67, 79, 97, 109, 121, 127, 139, 151, 157, 169, 181, 187, 199 (mod 210) ; dans $[3, 49]$: 19, 31, 37.

La densité de classes qui passent à travers tous les filtres vaut

$$\delta_n = \prod_{\substack{p \leq \sqrt{n} \\ p \nmid n}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \mid n \\ p \leq \sqrt{n}}} \left(1 - \frac{1}{p}\right),$$

et le produit central se factorise exactement :

$$\prod_{3 \leq p \leq x} \left(1 - \frac{2}{p}\right) = \underbrace{\prod_{3 \leq p \leq x} \left(1 - \frac{1}{p}\right)^2}_{\sim e^{-2\gamma} / \log^2 x} \times \underbrace{\prod_{3 \leq p \leq x} \frac{p(p-2)}{(p-1)^2}}_{\rightarrow 2C_2}, \quad (2)$$

où $C_2 \approx 0,66016$ est la constante des nombres premiers jumeaux : cribler les classes 0 et n modulo p est la même opération que cribler les classes 0 et 2 des jumeaux. La mire de Goldbach et la mire des jumeaux sont les mêmes enroulements. L'heuristique qui en résulte ($\asymp n / \log^2 n$ candidats) est correcte ; en faire une *minoration* passant la parité est exactement le problème ouvert.

5. Le théorème de Chen : jusqu'où le crible peut monter

Voici, en formules, ce que l'on sait réellement franchir - et pourquoi on s'arrête à P_2 .

Théorème 9 (Chen, 1973). *Tout entier pair n assez grand s'écrit $n = p + m$ avec p premier et m un P_2 (produit d'au plus deux premiers). De plus, le nombre de telles écritures satisfait*

$$\#\{p \leq n : p \text{ premier}, \Omega(n-p) \leq 2\} \geq c \cdot 2C_2 \prod_{2 < p|n} \frac{p-1}{p-2} \cdot \frac{n}{\log^2 n},$$

avec une constante explicite $c > 0$ (de l'ordre de 0,67 chez Chen ; à comparer à la série singulière de Hardy-Littlewood, qui donnerait le même facteur avec $c = 1$ pour les décompositions en deux premiers).

5.1. Esquisse, en quatre formules

(i) *Le changement de variable (l'échange)*. On ne crible plus tous les $m \leq n$, mais la séquence

$$\mathcal{A} = \{n - p : p \text{ premier}, p \leq n\},$$

en exigeant seulement que $n - p$ échappe aux petits facteurs. Pour chaque premier q , la condition $q \mid n - p$ élimine *une seule* classe, $p \equiv n \pmod{q}$: crible de dimension $\kappa = 1$, contre $\kappa = 2$ au § précédent (le facteur $1 - \frac{2}{p}$ disparaît au profit de $1 - \frac{1}{p}$).

(ii) *Le niveau de distribution*. Il faut la répartition des premiers dans les progressions arithmétiques, fournie par Bombieri-Vinogradov :

$$\sum_{q \leq D} \max_{(a,q)=1} \left| \pi(x; q, a) - \frac{\text{li}(x)}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x}, \quad D = \frac{\sqrt{x}}{\log^B x} :$$

niveau de distribution $\theta = 1/2$.

(iii) *Le crible linéaire*. Avec D le niveau, z la borne de criblage et $s = \frac{\log D}{\log z}$, les fonctions de Rosser-Jurkat-Richert $F(s) \geq f(s)$ encadrent

$$S(\mathcal{A}, z) = \#\{a \in \mathcal{A} : (a, P(z)) = 1\}, \quad P(z) = \prod_{q < z} q,$$

par $\left(\text{li}(n) \prod_{q < z} \left(1 - \frac{1}{q}\right) \right) \cdot f(s)$ et $\cdots F(s)$; et $f(s) = 0$ pour $s \leq 2$. Pour prouver que $n - p$ est premier, il faudrait cribler jusqu'à $z = \sqrt{n}$, donc $s \approx 1 < 2$: la borne inférieure s'effondre. C'est la parité, en formules : un crible de niveau $\frac{1}{2}$ ne peut pas certifier zéro facteur premier, ni distinguer $\Omega \leq 2$ de $\Omega \leq 3$.

(iv) *Les poids de Chen-Richert*. L'astuce de Chen : pondérer les nombres qui passent à travers tous les filtres de $z = n^{1/8}$ par

$$\Phi(m) = 1 - \frac{1}{2} \sum_{\substack{z < q|m \\ q \leq n^{1/3}}} 1 \quad (\text{plus termes correctifs}),$$

conçus pour que $\Phi(m) \leq 1$ si $\Omega(m) \leq 2$ et $\Phi(m) \leq 0$ si $\Omega(m) \geq 3$; la somme pondérée $\sum_p \Phi(n-p)$ minore donc le nombre d'écritures en P_2 , et se calcule par crible inférieur (majoration des termes corrects par crible *supérieur*, via l'échange et la fonction de Buchstab ω qui compte les entiers sans petit facteur premier). La constante 0,67 est le résultat de l'optimisation ; elle dépend aussi du possible *caractère exceptionnel* (zéro de Siegel) modulo un diviseur de n , qui fausse la répartition de $\pi(x; q, n \bmod q)$ près du niveau : c'est le même obstacle qui conditionne les résultats de type Linnik.

5.2. Lecture dans la mire

Exiger que $n-p$ soit premier, c'est exiger que le point d'arrivée $n-p$ n'atteigne *aucune* coche, d'aucun degré. Chen relâche : l'arrivée évite toutes les coches de petit degré ($q < z$), et peut se poser sur *au plus deux* coches de grand degré ($n-p = qq'$). Le crible de niveau $\frac{1}{2}$ sait certifier "au plus deux", jamais "aucune" : la barrière de parité, encore, désormais quantitative.

6. Conclusion

La mire est un dictionnaire fidèle : coches $\leftrightarrow$ fibres de points base, enroulements $\leftrightarrow$ revêtements (qui existent exactement quand $p \mid n$, le défaut de recollement étant $n \bmod p$), parcours $\leftrightarrow$ monodromie, candidats $\leftrightarrow$ relevés évitant les points de branchement. Mais ce dictionnaire est une équivalence de langages, pas un mécanisme d'existence : la non-vacuité des candidats pour tout n pair ≥ 6 reste le maillon manquant. Le théorème de Chen marque la frontière actuelle : avec le niveau $\frac{1}{2}$ de Bombieri-Vinogradov, on sait descendre à "au plus deux points de branchement rencontrés", et pas en dessous.

7. Annexes

Les cours suivants d'Étienne Ghys et Henri-Paul de Saint-Gervais à propos de la notion de revêtement :

Le groupe fondamental par les revêtements 1

<https://www.youtube.com/watch?v=q8z0KZwOLr8t=80s> .

Le groupe fondamental par les revêtements 2

<https://www.youtube.com/watch?v=zWpZIFCOZwU> .

Le groupe fondamental par les revêtements 3

<https://www.youtube.com/watch?v=4YAzdm1SW6A> .

Le groupe fondamental par les revêtements 4

<https://www.youtube.com/watch?v=nDeh82kXsdk> .

La page du site Analysis situ à ce propos :

<https://analysis-situs.math.cnrs.fr/Les-revetements.html> .

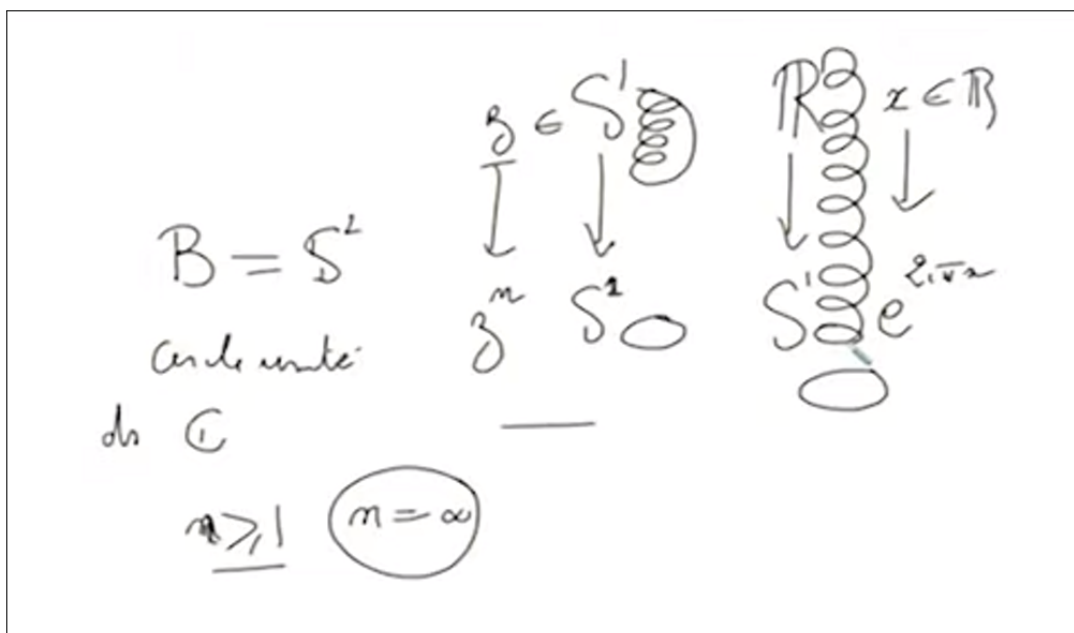


FIGURE 2 : Dessin capté lors du cours n° 1 d'Étienne Ghys au sujet des revêtements pour le site Analysis situ.

Références de Connes, Malgoire, Monique Hakim, Johnstone en lien avec le sujet

Alain Connes : Un topo sur les topes, 2017, dans le cadre du Colloque Lectures Grothendieckiennes à l'ENS.

<https://denisevellachemla.eu/2020-transc-ac-topo2.pdf> .

Alain Connes : Cohomologie cyclique et géométrie différentielle non-commutative, 1986, Congrès international des mathématiciens, Berkeley

<https://denisevellachemla.eu/2020-trad-topog.pdf> .

Jean Malgoire : Un héritage mathématique fertile, 2016, article du magazine Pour la Science, 2016, en hommage à Alexander Grothendieck dont Malgoire a été l'élève.

<https://denisevellachemla.eu/2019-transc-Malgoire.pdf> .

Monique Hakim : Topos annelés et schémas relatifs, 1972.

<https://denisevellachemla.eu/Hakim-Monique.pdf> .

P. T. Johnstone : Topos effondrés et variétés fermées cartésiennes,

<https://denisevellachemla.eu/2026-trad-br-Johnstone.pdf> .