

Topics in Mathematics for the Traveling Student

Laurent Bétermin, Markus Hausmann, Malte Leip,

Fabien Pazuki, Angélica Torres

March 21, 2020

Topics in Mathematics for the Traveling Student



Lecture notes
University of Copenhagen
2017–2019

Contents

| | |
|---|-----------|
| Preface | 5 |
| 1 ToMaTS Français | 9 |
| 1.1 Le principe des tiroirs de Dirichlet-Schläfli | 9 |
| 1.2 Géométrie fractale | 22 |
| 1.3 Autour de la formule d'Euler | 34 |
| 1.4 Topologie sur les espaces matriciels | 40 |
| 1.5 Calculs d'intégrales | 43 |
| 1.6 Notations | 46 |
| 1.7 Vocabulaire | 48 |
| 2 ToMaTS Español | 51 |
| 2.1 El principio del palomar | 51 |
| 2.2 Fractales | 62 |
| 2.3 Topología del espacio de matrices | 74 |
| 2.4 Vocabulario | 80 |
| 3 ToMaTS Deutsch | 83 |
| 3.1 Das Schubfachprinzip von Dirichlet | 83 |
| 3.2 Eulers Formel | 92 |
| 3.3 Der grosse Satz von Fermat | 102 |

Preface

The project called *Topics in Mathematics for the Traveling Student* (ToMaTS) emerged in the second half of 2017 from the Department of Mathematical Sciences, University of Copenhagen, where the five authors were employed during the two test years, 2017-2018 and 2018-2019. At that moment in time, the challenge we were facing was to adjust to the following situation.

- (i) Undergraduate students were in demand of some initiative to help them seize the opportunity of spending some time studying abroad.
- (ii) Bachelor courses were all given in Danish.
- (iii) At the research level, more and more international colleagues were joining the Department of Mathematical Sciences.
- (iv) Most post-doctoral contracts involved a reasonable but non-trivial teaching load.

An idea came up naturally: how about having some mathematics courses given by international colleagues in their native language, directed at Danish students who are preparing for a period abroad? A quick glance at the countries that were represented in the post-doc community at the Department of Mathematical Science of the University of Copenhagen on the one hand, and at the European countries that were the target for international exchanges in previous years on the other hand, led to the following choice in autumn 2017: let's ask Laurent Bétermin to give mathematical lectures in French, Markus Hausmann to give mathematical lectures in German, and Angélica Torres to give mathematical lectures in Spanish!

We were lucky to gain quick and frank support from the direction of the Department of Mathematical Science, many thanks for letting us carry on with this experiment.

So we opened three courses in parallel, French track, German track, Spanish track. Open to everyone, math students, but also other students willing to see mathematics in action in a different language, as well as staff members, professors, anyone interested, really. The courses were given for two hours a week, every Friday from 13:00 to 15:00, in three different classrooms. No exams, no grades, no homeworks, no pressure. A moment of pure joy and fun, discovering mathematics and a foreign language at the same time!

Who were the students? Most of the people who signed up were bachelor students, but we also got some master students, PhD students, and even staff members! Obvious challenge: the level of the course... both in mathematics and in the foreign language. We took a reasonable approach: adjust to the audience's level in mathematics when possible, and keep the whole course in the foreign language. The planned mathematical content is the content described in the following course notes, but some adjustments were made when deemed necessary.

Great success from day one, which is clearly due to the fact that the team was very motivated by the project and gave nice and friendly lectures: merci, danke, gracias!

In autumn 2018, the French track was kept by Laurent Bétermin, the Spanish track by Angélica Torres, and the German track was passed from Markus Haussman to Malte Leip. Many thanks to all of them, with a particular mention to Laurent Bétermin: not only for the tremendous work he accomplished on the French track, but also because of the inspiration he gave to the others!

In releasing these notes, we very much hope that they will inspire other courses of the same type across European universities, henceforth giving new perspectives on the Erasmus program!

The content varies slightly from one track to the other. These notes begin with the French track, where we start by covering some applications of the pigeonhole principle, an introduction to fractal geometry, mathematics around Euler's formula, topology for matrices, and explicit computations of integrals. It also contains some details about vocabulary and notation in French in the last paragraphs. We move on to the Spanish track, where we also start with the pigeonhole prin-

principle, fractal geometry, topology for matrices, and vocabulary notes. Finally the German track, with the common pigeonhole principle, Euler's formula, an introduction to Fermat's Last Theorem and the *abc*-conjecture.

Mathématiquement vôtre,

Fabien Pazuki,
University of Copenhagen,
January 27, 2019.

Chapitre 1

ToMaTS Français

1.1 Le principe des tiroirs de Dirichlet-Schläfli

Appelé *Schubfachprinzip* (principe des tiroirs) par Johann Peter Gustav Lejeune Dirichlet (1805-1859) en 1834, il est nommé *pigeonhole principle* (principe des casiers à pigeons) en anglais. Il est communément énoncé de la façon suivante :

Si n chaussettes occupent m tiroirs et si $n > m$, alors au moins un tiroir doit contenir strictement plus d'une chaussette.



FIGURE 1.1 : Tiroirs et chaussettes

1.1.1 Énoncé et preuve

Proposition 1 (Principe des tiroirs de Dirichlet–Schläfli). Soit $f : A \rightarrow B$ une application entre deux ensembles finis. Posons $n = |A|$ et $m = |B|$.

- (i) Si $n > m$, alors il existe $b \in B$ tel que $|f^{-1}(\{b\})| \geq 2$.
- (ii) Plus généralement, si il existe $r \in \mathbb{N}$ tel que $n > rm$, alors il existe $b \in B$ tel que $|f^{-1}(\{b\})| \geq r + 1$.

Démonstration. Montrons (ii). Soit $r \in \mathbb{N}$ tel que $n > rm$. On raisonne par l'absurde et on suppose que $|f^{-1}(\{b\})| \leq r$ pour tout $b \in B$. Comme on a

$$A = \bigsqcup_{b \in B} f^{-1}(\{b\}),$$

on obtient

$$n = |A| = \sum_{b \in B} |f^{-1}(\{b\})| \leq r|B| = mr,$$

ce qui contredit notre hypothèse. Ainsi, il existe $b \in B$ tel que $|f^{-1}(\{b\})| \geq r + 1$. \square

Remarque 2 (Analogie). L'analogie avec les chaussettes et les tiroirs est donc la suivante :

- A est l'ensemble des chaussettes,
- B est l'ensemble des tiroirs,
- f est la façon de disposer les chaussettes dans les tiroirs.

Remarque 3 (Image réciproque). On dit que $f^{-1}(C)$ est l'image réciproque de l'ensemble C par f .

Remarque 4 (Injectivité). En particulier, (i) signifie qu'il ne peut pas y avoir d'application injective entre A et B tels que $|A| > |B|$.

Remarque 5 (Entiers naturels). Rappelons qu'en France l'ensemble des nombres entiers naturels est $\mathbb{N} := \{0, 1, 2, \dots\}$, et donc que $\mathbb{N}^* = \{1, 2, \dots\}$. De plus, pour tout $a, b \in \mathbb{N}$ tels que $a < b$, on peut noter $\llbracket a, b \rrbracket := [a, b] \cap \mathbb{N}$ l'ensemble des nombres entiers naturels compris entre a et b .

Remarque 6 (Différence entre application et fonction). Rappelez-vous la différence qu'il y a entre une fonction et une application. Une fonction $f : A \rightarrow B$ n'est pas nécessairement définie sur l'ensemble A en entier, mais sur son ensemble de définition $D_f \subset A$. Une application $f : A \rightarrow B$ est définie sur A tout entier.

Remarque 7 (Logique et raisonnement). Si on souhaite démontrer que $P \implies Q$, on peut vouloir le faire :

- **par contraposition**, en montrant que $\text{non}(Q) \implies \text{non}(P)$;
- **par l'absurde**, en montrant qu'il existe une propriété R pour laquelle on puisse établir à la fois $\text{non}(Q) \implies R$ et $P \implies \text{non}(R)$ de façon à conclure que $\text{non}(Q)$ est impossible.

Evidemment, quand $R = \text{non}(P)$, les deux raisonnements sont les mêmes, ce qui est le cas dans la preuve de la Proposition 1.

Voici un exemple où l'on voit clairement apparaître la propriété R , différente de la propriété $\text{non}(P)$. On souhaite montrer que si n^2 est pair (propriété P), alors n est pair (propriété Q). On suppose que n est impair (c'est-à-dire que l'on suppose $\text{non}(Q)$), alors $n + 1$ est pair ainsi que $(n + 1)^2$, c'est-à-dire que $n^2 + 2n + 1$ est pair (et on appelle R cette propriété). Or, comme n^2 est pair (c'est la propriété P), on a que $n^2 + 2n + 1$ est impair (c'est-à-dire $\text{non}(R)$), ce qui est absurde. Donc n est nécessairement pair.

1.1.2 Applications directes

Avec ce principe, il est possible de démontrer plusieurs résultats amusants.

Exemple 8. A Paris, il existe au moins 11 personnes ayant exactement le même nombre de cheveux.



FIGURE 1.2 : Foule parisienne devant la Basilique du Sacré Coeur de Montmartre

Solution : Cela découle du principe des tiroirs car la population de Paris est supérieure à $n = 2141000$ habitants et le nombre de cheveux ne dépasse pas $m = 200000$.

Ainsi, si les tiroirs désignent les possibilités pour le nombre de cheveux et les chaussettes désignent les habitants de Paris, alors d'après le principe des tiroirs, comme $n > 10m$ ($r = 10$), au moins $10 + 1 = 11$ habitants auront le même nombre de cheveux.

Exemple 9 (cf. [15]). Combien de rois peut-on placer sur un échiquier (8x8) de manière à ce qu'aucun roi n'attaque un autre ?

Solution : On découpe l'échiquier en 16 secteurs carrés formés de 4 cases. Supposons qu'il y ait plus de 17 rois sur l'échiquier, alors par le principe des tiroirs, il y aura un des secteurs qui contiendra au moins deux rois, et ainsi ils s'attaqueront l'un l'autre. La réponse est donc 16.

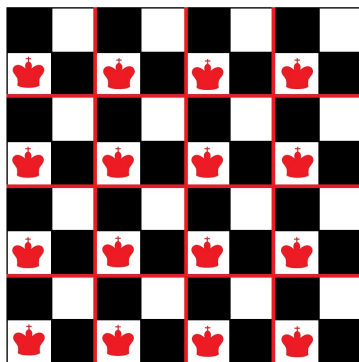


FIGURE 1.3 : Echiquier

Exemple 10. On jette de la peinture noire au hasard sur un tableau blanc de taille $2m \times 2m$. Montrer qu'il existe toujours deux points de la même couleur espacés exactement de 1 mètre.

Solution : Sur ce tableau, il est toujours possible de construire un triangle équilatéral de côté 1 mètre. Comme ce triangle a trois sommets et qu'il n'y a que deux couleurs possibles, deux des sommets ont la même couleur d'après le principe des tiroirs.

Exemple 11. On considère 5 points $A_1, \dots, A_5 \in \mathbb{Z}^2$. Montrer qu'il existe deux de ces points A_i, A_j tels que le milieu du segment $[A_i, A_j]$ appartient à \mathbb{Z}^2 .

Solution : On rappelle que les coordonnées du milieu d'un segment $[A, B]$, où $A(x_A, y_A)$ et $B(x_B, y_B)$ sont $(x_A + x_B)/2$ et $(y_A + y_B)/2$. On raisonne sur la parité

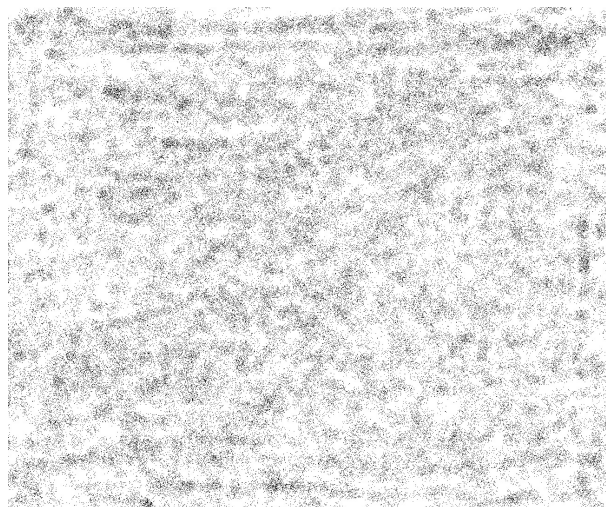
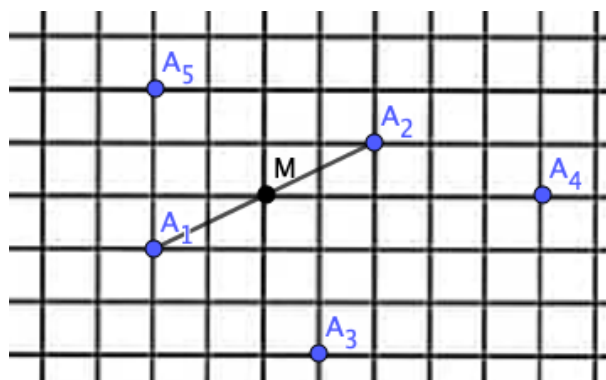


FIGURE 1.4 : Tableau blanc couvert de peinture noire

FIGURE 1.5 : Tout ensemble constitué de cinq points de \mathbb{Z}^2 contient toujours une paire dont le milieu est aussi un point de \mathbb{Z}^2

des coordonnées et on définit :

$$\begin{aligned}
 S_{PP} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z}, y \in 2\mathbb{Z}\} \\
 S_{PI} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z}, y \in 2\mathbb{Z} + 1\} \\
 S_{II} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z} + 1, y \in 2\mathbb{Z} + 1\} \\
 S_{IP} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z} + 1, y \in 2\mathbb{Z}\}.
 \end{aligned}$$

Par le principe des tiroirs, comme on a 5 points et 4 ensembles, il existe $A_i(x_i, y_i)$ et $A_j(x_j, y_j)$ qui appartiennent au même ensemble. Ainsi, on a $x_i + x_j \in 2\mathbb{Z}$ et $y_i + y_j \in 2\mathbb{Z}$ et le milieu de $[A_i, A_j]$ appartient à \mathbb{Z}^2 .

Exemple 12. On place au hasard 5 points sur une sphère. Montrer que l'on peut toujours séparer la sphère en deux parties de même surface telles qu'au moins 4 points appartiennent au même domaine, en supposant qu'un point de la frontière entre ces deux parties appartient aux deux parties en même temps.

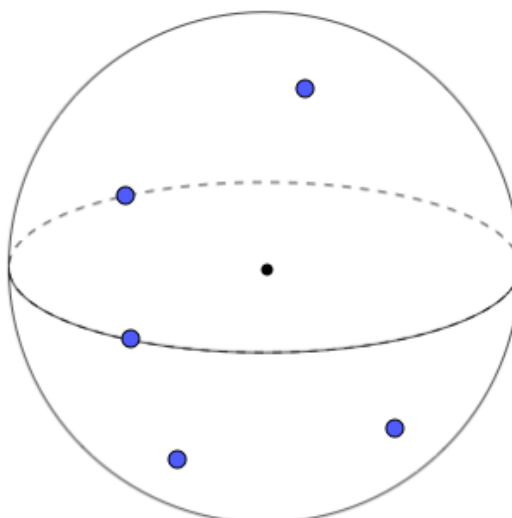


FIGURE 1.6 : Cinq points sur une sphère

Solution : Il suffit de prendre deux points au hasard parmi ces 5 points et de tracer le grand cercle passant par ces deux points. Il reste donc 3 points qui sont répartis sur deux domaines. Par le principe des tiroirs, il existe donc un domaine contenant au moins 2 de ces points, et donc contenant au moins 4 points au total en comptant les deux points appartenant à la frontière.

Exemple 13 (Nombre de Ramsey - un exemple concret simple). Dans une soirée avec (au moins) 6 personnes, montrer qu'il y a toujours trois personnes qui se connaissent ou bien trois personnes qui ne se connaissent pas les uns les autres.

Solution : Soient 6 points du plan $x_1, \dots, x_6 \in \mathbb{R}^2$ correspondants à ces 6 personnes. Si deux personnes se connaissent, traçons un segment bleu entre leurs points respectifs, sinon traçons un segment vert. Il y a 5 segments partants de x_1 , tracés de deux couleurs différentes. Ainsi, par le principe des tiroirs (appliqué à $n = 5$, $m = 2$ et $r = 2$), il existe au moins 3 segments de la même couleur. Supposons que ces segments relient x_1 à x_2, x_3 et x_4 . On a maintenant deux possibilités :

- soit l'un des segments $[x_2, x_3]$, $[x_3, x_4]$ ou $[x_2, x_4]$ est bleu, et on a un triangle bleu, ce qui signifie que trois personnes se connaissent les uns les autres,

- soit aucun de ces segments n'est bleu, et ainsi le triangle $x_2x_3x_4$ est vert, ce qui signifie que trois personnes ne se connaissent pas les uns les autres.

Exemple 14 (Mathematics competitions 4-7 grade, Regalia 6, Sofia (1993). cf. [3]). Un triangle équilatéral ABC et un carré $MNPQ$ sont inscrits dans un cercle de périmètre s . Aucun des sommets du triangle ne coïncide avec un sommet du carré. Ainsi, ces sommets divisent le cercle en 7 arcs. Montrer qu'au moins un de ces arcs a une longueur plus petite que $s/24$.

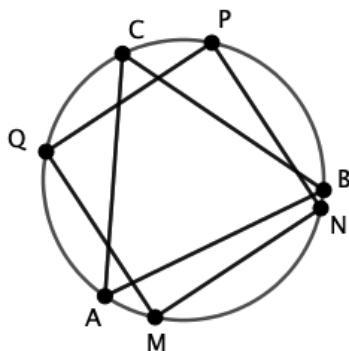
Solution : Les sommets du triangle divisent le cercle en 3 arcs et le carré a 4 sommets, donc, par le principe des tiroirs, il existe au moins un arc de cercle entre deux sommets du triangle qui contient 2 des sommets du carré. Supposons que les sommets M et N appartiennent à l'arc \widehat{AB} . Notons $\ell(XY)$ la longueur de l'arc \widehat{XY} , on obtient

$$\ell(AB) = \frac{s}{3} \quad \text{and} \quad \ell(MN) = \frac{s}{4},$$

et donc

$$\ell(AM) + \ell(NB) = \frac{s}{3} - \frac{s}{4} = \frac{s}{12}.$$

Ainsi, un des arcs \widehat{AM} ou \widehat{NB} a une longueur plus petite que $s/24$.



Exemple 15 (Un principe des tiroirs "infini"). Pour tout $c \in \mathbb{Q}_+^* \setminus \{1\}$, il existe $a, b \in \mathbb{R} \setminus \mathbb{Q}$ tels que $c = a^b$.

Solution : Soit $c \in \mathbb{Q}_+^* \setminus \{1\}$, alors on définit f_c qui associe à chaque $a > 0$ la solution b de l'équation $a^b = c$. Cette application est injective car $f_c(a) = f_c(a') \iff \frac{\ln(c)}{\ln(a)} = \frac{\ln(c)}{\ln(a')} \iff a = a'$ par l'injectivité du logarithme. Si maintenant on restreint cette application aux irrationnels positifs et que l'on suppose que pour tout $a \in \mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$, il n'existe aucun $b \in \mathbb{R} \setminus \mathbb{Q}$ tels que $a^b = c$, alors

$f_c : \mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty) \rightarrow B \subset \mathbb{Q}$ est injective. Comme le cardinal de $\mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$ est plus grand que celui de B – car \mathbb{Q} est dénombrable et $\mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$ ne l'est pas –, c'est impossible et le résultat est démontré.

Exemple 16 (Un résultat de Vázsonyi et Sved. Voir [2]). Le résultat suivant est une des plus belles applications du principe des tiroirs. Soient n entiers naturels non-nuls a_1, \dots, a_n , distincts ou non. Montrer qu'il existe toujours un ensemble de nombres consécutifs $a_{k+1}, a_{k+2}, \dots, a_\ell$ dont la somme $\sum_{i=k+1}^{\ell} a_i$ est un multiple de n .

Solution : Posons $A = \{0, a_1, a_1 + a_2, \dots, a_1 + a_2 + \dots + a_n\}$ et $B = \{0, 1, \dots, n-1\}$. Considérons l'application $f : A \rightarrow B$ où $f(m)$ est le reste de m dans la division euclidienne par n . Puisque $|A| = n+1 > n = |B|$, il existe deux sommes $a_1 + \dots + a_k$ et $a_1 + \dots + a_\ell$ ($k < \ell$) ayant le même reste dans la division par n , la première somme pouvant être la somme vide valant 0. Ainsi, la somme

$$\sum_{i=k+1}^{\ell} a_i = \sum_{i=1}^{\ell} a_i - \sum_{i=1}^k a_i$$

a pour reste 0 dans la division par n , ce qui conclut la démonstration.

1.1.3 Le théorème d'approximation de Dirichlet

Les deux premières sections de cette partie sont issues de [6].

Enoncé et preuve du théorème

Théorème 17 (Dirichlet). Soit $\alpha \in \mathbb{R}$ et $N \in \mathbb{N}_+$. Alors il existe $q \in \{1, \dots, N\}$ and $p \in \mathbb{N}$ tels que

$$|q\alpha - p| < \frac{1}{N}.$$

Démonstration. Pour tout $i \in \{0, 1, \dots, N\}$, on définit

$$\beta_i := i\alpha - [i\alpha],$$

où $[x]$ désigne la partie entière de x , c'est-à-dire le plus grand entier plus petit ou égal à x . En particulier, on a $[x] \leq x < [x] + 1$. On en déduit que

$$0 \leq \beta_i < 1.$$

Pour tout $k \in \{1, 2, \dots, N\}$, on définit l'intervalle $S_k := \left[\frac{k-1}{N}, \frac{k}{N} \right)$. Il est clair que $[0, 1)$ est l'union disjointe des intervalles S_1, \dots, S_N . Par le principe des tiroirs, au

moins deux des nombres β_0, \dots, β_N appartiennent au même intervalle S_k pour un certain $k \in \{1, 2, \dots, N\}$. Supposons que $\beta_i, \beta_j \in S_k$ où $0 \leq i < j \leq N$, alors on a

$$-\frac{1}{N} < \beta_i - \beta_j = (j - i)\alpha - (\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor) < \frac{1}{N}.$$

Le théorème est prouvé car $1 \leq q := j - i \leq N$ et $p := \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor \in \mathbb{N}$. \square

Critère d'irrationalité

Le but de cette section est d'établir un critère d'irrationalité pour les nombres réels.

Proposition 18. Un nombre α est irrationnel si et seulement si il existe deux suites d'entiers $(p_n)_n$ et $(q_n)_n$ telles que

$$\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$$

et $q_n \alpha - p_n \neq 0$ pour tout n .

Démonstration. Supposons que α est irrationnel. Alors, par le Théorème 17, pour tout $n \in \mathbb{N}^*$, il existe des entiers p_n et q_n tels que $1 \leq q_n \leq n$ et

$$|q_n \alpha - p_n| < \frac{1}{n}.$$

On en déduit que $\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$ et que, pour tout n , $q_n \alpha - p_n \neq 0$ car α est irrationnel.

Réciproquement, supposons qu'il existe $(p_n)_n$ et $(q_n)_n$ tels que $\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$ et que, pour tout n , $q_n \alpha - p_n \neq 0$. On raisonne par l'absurde et on suppose que $\alpha \in \mathbb{Q}$ et s'écrit $\alpha = \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ et $b > 0$. On a donc

$$|q_n \alpha - p_n| = \left| \frac{q_n a - p_n b}{b} \right| \geq \frac{1}{b}$$

car $q_n \alpha - p_n \neq 0$ pour tout n . Cela contredit le fait que $\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$ et donc α est irrationnel. \square

Maintenant, appliquons ce résultat.

Corollary 19. Le nombre $\sqrt{2}$ est irrationnel.

Démonstration. On développe $(\sqrt{2} - 1)^n$ et, comme $(\sqrt{2})^2 = 2$, on obtient, pour tout $n \in \mathbb{N}$,

$$(\sqrt{2} - 1)^n = q_n \sqrt{2} - p_n,$$

où $p_n, q_n \in \mathbb{N}$. On a

$$\lim_{n \rightarrow +\infty} q_n \sqrt{2} - p_n = \lim_{n \rightarrow +\infty} (\sqrt{2} - 1)^n = 0$$

car $|\sqrt{2} - 1| < 1$. De plus,

$$q_n \sqrt{2} - p_n = (\sqrt{2} - 1)^n \neq 0$$

pour tout $n \in \mathbb{N}$ car $\sqrt{2} \neq 1$. Par la Proposition 18, on en déduit que $\sqrt{2}$ est irrationnel. \square

Série divergente

Le but de cette partie, inspirée de [17, 14], est de montrer comment le théorème d'approximation de Dirichlet permet de prouver qu'une série diverge. On commence par montrer le lemme suivant qui est un complément au Théorème 17.

Lemme 20. Soit α irrationnel, alors Il existe une infinité de couples d'entiers (p, q) tels que

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Démonstration. Par le Théorème 17, on sait que si α est irrationnel, pour tout $N \in \mathbb{N}_+$, il existe $q \in \{1, \dots, N\}$ et $p \in \mathbb{N}$ tels que

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

Montrons que l'ensemble des couples (p, q) satisfaisants cette propriété est infini. Raisonnons par l'absurde et supposons qu'il en existe un nombre fini $C = \{(p_i, q_i)\}_{1 \leq i \leq r}$. On définit

$$\epsilon := \min_i \left\{ \left| \alpha - \frac{p_i}{q_i} \right| \right\}.$$

Comme $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\epsilon > 0$. Ainsi, il existe $N_0 > 0$ tel que $\epsilon > \frac{1}{N_0}$. Appliquons maintenant le Théorème 17 à ce nombre N_0 et à α , il existe donc (p_0, q_0) tels que

$$\left| \alpha - \frac{p_0}{q_0} \right| < \frac{1}{N_0 q_0} \leq \frac{1}{N_0} < \epsilon.$$

Ainsi, $(p_0, q_0) \in C$ et le fait que $\left| \alpha - \frac{p_0}{q_0} \right| < \epsilon$ est une contradiction. Ainsi, le cardinal de C est infini et le résultat est démontré. \square

Proposition 21. La série $\sum_{n=1}^{\infty} \frac{1}{n^2 \sin^2(n)}$ est divergente.

Démonstration. Par le Lemme 20, comme π est irrationnel, il existe une infinité d'entiers naturels n, q tels que

$$\left| \pi - \frac{n}{q} \right| < \frac{1}{q^2}.$$

Cela implique qu'il existe une infinité d'entiers naturels n, q tels que $\pi - n/q > -1/q^2$ et, comme $q \geq 1$, il existe une infinité d'entiers naturels n, q tels que

$$\frac{n}{q} < \pi + \frac{1}{q^2} \leq \pi + 1.$$

On a donc, pour tout n, q dans cet ensemble

$$|\sin n| = |\sin(n - q\pi)| \leq |n - q\pi| < \frac{1}{q} = \frac{1}{n} \frac{n}{q} < \frac{\pi + 1}{n}.$$

Il existe donc une infinité d'entiers naturels n tels que

$$\frac{1}{n^2 \sin^2(n)} > \frac{1}{(1 + \pi)^2},$$

et la série de terme principal $\frac{1}{n^2 \sin^2(n)}$ diverge. □

1.1.4 Théorème de Hall (lemme des mariages)

Le but de cette partie est de démontrer le Théorème de Hall, énoncé pour la première fois par le mathématicien anglais Philip Hall (1904-1982). Vous pouvez consulter [19] pour plus d'informations.

Définition 22. Soit X un ensemble et S une famille de sous-ensembles finis de X , non-nécessairement distincts, et comptés avec multiplicité.

Un système de représentants distincts de S est l'image d'une application injective $f : S \rightarrow X$ telle que, pour tout $s \in S$, $f(s) \in s$.

On dit que S satisfait la condition de mariage si, pour toute sous-famille $W \subset S$,

$$|W| \leq \left| \bigcup_{A \in W} A \right|.$$

Remarque 23. Cela signifie que f sélectionne un représentant de chaque $s \in S$ de telle sorte que tous les représentants soient distincts les uns des autres.

De plus, S satisfait la condition de mariage si toute sous-famille W de S contient au moins $|W|$ différents membres de X .

Théorème 24 (Hall, 1935, Condition nécessaire). Soit S une famille. S'il existe un système de représentants distincts pour S , alors S satisfait la condition de mariage.

Démonstration. Montrons que s'il existe un système de représentants distincts pour S , alors S satisfait la condition de mariage. L'autre implication ne sera pas montrée ici. Pour cela, montrons la contraposée, c'est-à-dire que si S ne satisfait pas la condition de mariage, alors il n'existe pas de système de représentants distincts pour S .

Si S ne satisfait pas la condition de mariage, alors il existe une sous-famille $W_0 \subset S$ telle que

$$|W_0| > \left| \bigcup_{A \in W_0} A \right|.$$

Raisonnons par l'absurde et supposons qu'il existe un système de représentants distincts $f(S)$ pour S . Alors par définition, la restriction $f|_{W_0} : W_0 \rightarrow \bigcup_{A \in W_0} A$ est injective. Par le principe des tiroirs, comme $|W_0| > \left| \bigcup_{A \in W_0} A \right|$, c'est impossible. Ainsi, il n'existe pas une telle application f si S ne satisfait pas la condition de mariage, et le résultat est prouvé. \square

Remarque 25. La réciproque est aussi vraie, ce qui complète le Théorème de Hall. La preuve n'est pas traitée dans ce cours. Un bon exercice serait de la traduire en français à partir de la page Wikipedia (section Graph theoretic formulation) du théorème.

Remarque 26 (Interprétation en terme de mariage). Etant données n filles et A_k étant l'ensemble des prétendants de la k -ième fille, alors le fait que $S = \{A_1, \dots, A_n\}$ satisfait la condition de mariage est équivalent avec le fait qu'il existe un mariage collectif des n filles, chacune avec un de leurs prétendants.

1.1.5 Exercices : Vocabulaire

Exercice 27. Compléter les phrases suivantes :

- (i) $f : A \rightarrow B$ une $|A| > |B|$, f n'est pas
- (ii) On que n est pair, n^2 est pair.
- (iii) Si x est, alors il $p, q \in \mathbb{Z}$
 $x = p/q$.
- (iv) $f^{-1}(B)$ est appelée de l'..... B par f .
- (v) Si $A(x_A, y_A) \in \mathbb{R}^2$ et $B(x_B, y_B) \in \mathbb{R}^2$, alors le M qui a pour
..... $\left(\frac{x_A+x_B}{2}, \frac{y_A+y_B}{2}\right)$ est le du $[AB]$.

Exercice 28. Le but de cet exercice est de montrer qu'il existe deux nombres irrationnels a, b tels que a^b est rationnel.

1. Montrer que $\sqrt{2}$ est irrationnel.
2. Compléter la phrase suivante : $\sqrt{2}^{\sqrt{2}}$ est, alors le résultat est Il suffit de $a = \dots$ et $b = \dots$
3. Compléter la phrase suivante : Inversement, si $\sqrt{2}^{\sqrt{2}}$ est, alors on $a = \dots$ et $b = \dots$, et $a^b = \dots$ est

Remarque : En fait, $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$, c'est le Théorème de Gelfond-Schneider.

Exercice 29. Ecrire en toutes lettres les expressions mathématiques suivantes :

(i) $x \in A$

(ii) $\forall y \in \mathbb{R}$

$$(iii) \exists x \in \mathbb{R} \setminus \mathbb{Q}$$

$$(iv) \forall p \in \mathbb{Q}, \forall \eta \in \mathbb{R}_+^*, \exists r \in \mathbb{R} \setminus \mathbb{Q}, p < r < p + \eta$$

1.2 Géométrie fractale

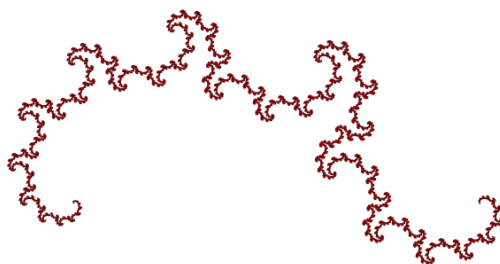
Dans son article [10] intitulé *How long is the coast of Britain? Statistical self-similarity and fractional dimension (Science, 1967)*, le mathématicien Benoît Mandelbrot (1924-2010) popularisa la notion d'objet fractal, expliquant la nécessité de définir une dimension fractionnaire pour certains objets géométriques que l'on trouve dans la nature (par exemple les frontières de la France).



FIGURE 1.7 : Frontières de la France

Alors qu'il est intuitivement clair que le segment $[0, 1]$ a pour longueur 1 et dimension 1, qu'en est-il pour une courbe comme celle-ci ?

Si vous faites un zoom sur une des branches de \mathcal{C} , vous pouvez retrouver exactement la même forme que celle de \mathcal{C} . C'est ce que l'on appelle un objet autosimilaire. Il est ainsi extrêmement compliqué de déterminer sa longueur qui pourrait bien être infinie. Pire encore, ses irrégularités en font une courbe très éloignée d'une parabole ou de tout autre courbe régulière. Ainsi, on ne peut pas vraiment dire que la dimension de \mathcal{C} est 1. Elle devrait être supérieure à 1 (en fait elle vaut environ 1.5).

FIGURE 1.8 : Courbe du dragon \mathcal{C}

De même, que penser de la *courbe de Gosper* découverte par Bill Gosper en 1973? Elle est construite en remplaçant chaque segment par sept autres d'une longueur réduite de $7^{-1/2}$. Elle finit par remplir le plan en entier et sa dimension tend donc vers 2 quand le nombre d'étapes tend vers l'infini.

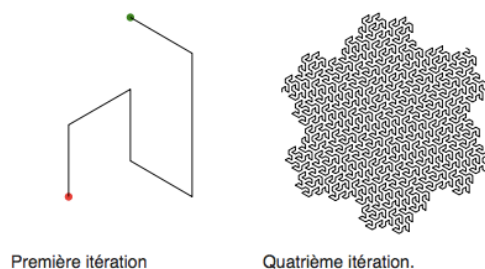


FIGURE 1.9 : Courbe de Gosper (source : Internet)

Ces objets irréguliers apparaissent dans la nature. Pensez à la surface d'un chou-fleur, un brocoli, celle d'un cerveau humain ou tout simplement un arbre. On aimerait ainsi être capable de “mesurer” de tels objets et d'en connaître leur dimension.

L'objectif de ce chapitre est de comprendre, à partir de la notion de mesure, comment l'on peut définir la dimension d'objets compliqués comme ceux-ci. Après avoir donné la définition abstraite d'une mesure, on s'appuiera sur l'intuition pour définir une dimension fractale “de boîtes”. On calculera les dimensions fractales d'objets fractals classiques, et enfin on définira les mesures et dimension de Hausdorff.

1.2.1 Les notions de mesure et de dimension

L'essentiel des résultats et concepts présentés dans cette partie sont issus de [7].



FIGURE 1.10 : Chou-fleur Romanesco et un arbre

Mesure

Si on souhaite donner une mesure à un objet géométrique (longueur, volume, etc.) plongé dans \mathbb{R}^n , alors on doit définir une application $\mu : \mathcal{B} \subset \mathbb{R}^n \rightarrow [0, +\infty]$, où \mathcal{B} est l'ensemble des parties mesurables de \mathbb{R}^n . Une telle mesure doit donc nécessairement satisfaire la propriété suivante :

μ est, c'est-à-dire que si $A \cap B = \emptyset$, $\mu(A \cup B) = \dots\dots\dots$

De plus, l'ensemble \mathcal{B} doit être une σ -algèbre, c'est-à-dire un sous-ensemble de $\mathcal{P}(\mathbb{R}^n)$ tel que

- (i) $\in \mathcal{B}$;
- (ii) $B \in \mathcal{B} \Rightarrow \dots\dots\dots$;
- (iii) Pour toute famille $(A_k)_{k \in \mathbb{N}}$, $\in \mathcal{B}$.

La vraie définition d'une mesure est donnée ici :

Définition 30. Soit S un ensemble et \mathcal{B} une σ -algèbre sur S . Une fonction $\mu : \mathcal{B} \rightarrow [0, \infty]$ est appelée une mesure si

- (i) $\mu(\emptyset) = \dots\dots\dots$,
- (ii) μ est σ -additive, c'est-à-dire que pour toute famille d'ensembles disjoints $\{B_n\} \subset \mathcal{B}$, on a

$$\mu \left(\bigcup_{n=1}^{\infty} B_n \right) = \dots\dots\dots$$

Dimension

On peut voir que la notion de dimension d'un objet est intimement liée à la notion de changement d'échelle. On connaît la propriété suivante :

Si on multiplie les distances d'un ensemble E de dimension $d(E)$ par ϵ , alors sa mesure est multipliée par

Ainsi, intuitivement, on a $d(E) = \dots\dots\dots$

De plus, quand ϵ est petit, alors la quantité $\frac{\mu(E)}{\mu(\epsilon E)}$ peut être vue comme le plus petit nombre de boîtes cubiques de côté ϵ nécessaires pour
 E . On notera $N_\epsilon(E)$ ce nombre. Si E est vraiment un ensemble simple, on retrouve les dimensions $d(E)$ que l'on connaît déjà :

- (i) Si $E = [0, 1]$, alors il faut $N_\epsilon(E) = \dots\dots\dots$ segments de longueur
 pour recouvrir parfaitement E , ainsi

$$d(E) = \dots\dots\dots$$

- (ii) Si $E = [0, 1]^2$, alors il faut $N_\epsilon(E) = \dots\dots\dots$ carrés de longueur
 pour recouvrir parfaitement E , ainsi

$$d(E) = \dots\dots\dots$$

Et cet exemple se généralise à $E = [0, 1]^n$ qui a donc pour dimension

$$d(E) = \dots\dots\dots$$

Mais si l'objet est beaucoup plus, il n'est pas réellement possible que le recouvrement corresponde exactement à l'objet. Par contre, cela devrait être le cas quand ϵ est infiniment

Ainsi, la **dimension de Bouligand-Minkowski** (appelée aussi "dimension de boîtes") est

$$\dim_B(E) = \lim_{\epsilon \rightarrow 0} \frac{\log N_\epsilon(E)}{-\log \epsilon}.$$

où $N_\epsilon(E)$ est le plus petit nombre de boîtes cubiques de côté ϵ nécessaires pour recouvrir E . De plus, le recouvrement par des boîtes de taille ϵ est appelé ϵ -recouvrement.

Remarque 31. Cette limite n'existe pas forcément. Ainsi on peut définir les dimensions supérieures et inférieures en remplaçant la limite par \limsup ou \liminf .

Nous allons maintenant calculer la dimension de boîtes d'objets fractals célèbres. Ensuite, nous introduirons les mesures et dimension de Hausdorff.

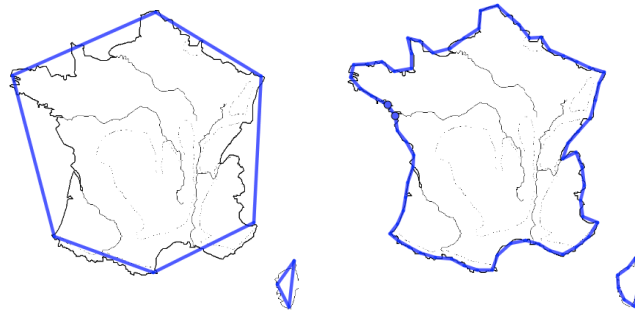


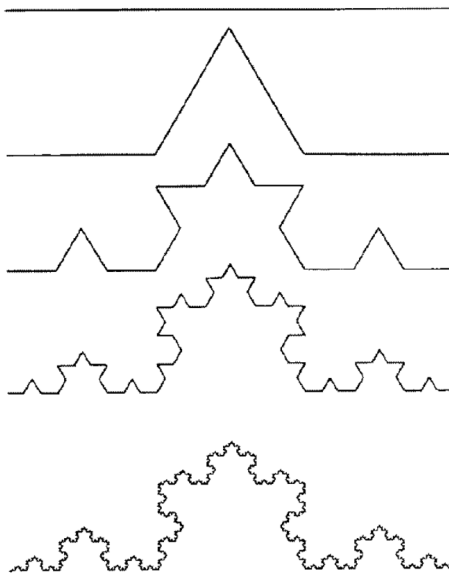
FIGURE 1.11 : Mesure des frontières de la France : plus la longueur ϵ est petite, plus on peut calculer précisément sa longueur et sa dimension.

1.2.2 Quelques exemples célèbres

Dans la suite, nous allons construire des objets fractals par récurrence, c'est-à-dire que l'on construira une famille d'objets $\{E_n\}$ qui converge vers un objet F . Il sera implicite que le ϵ -recouvrement de l'objet E_n par des boîtes de taille ϵ_n recouvre aussi F .

La courbe de Koch

Cette courbe a été étudiée par le mathématicien suédois Helge von Koch (1870-1924) en 1904. A l'origine, elle a été introduite comme exemple de "courbe continue sans tangente, obtenue par une construction géométrique élémentaire".



Principe de construction :

- (i) E_0 est un segment de longueur 1.
- (ii) Pour obtenir E_{n+1} , on divise chaque segment de E_n en trois parties égales et on remplace le tiers du milieu par un triangle équilatéral dont on supprime la base.
- (iii) On continue ce processus à l'infini, i.e. $F = \lim_{n \rightarrow +\infty} E_n$.

La longueur de E_n est Ainsi, la longueur de F est

A l'étape n , il faut $N_{\epsilon_n}(E_n) = \dots\dots$ boîtes de taille $\epsilon_n = \dots\dots\dots$ afin de recouvrir E_n . On a donc

$$\dim_B(F) = \dots\dots\dots$$

Si E_0 est remplacé par un triangle équilatéral de longueur 1, alors le même processus admet pour limite le **flocon de Koch** dessiné ci-dessous, qui a la même dimension de boîtes que F .

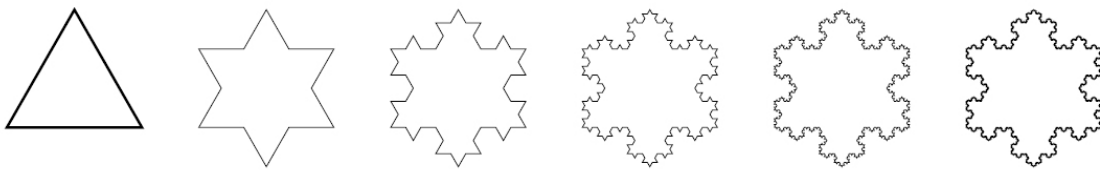


FIGURE 1.12 : Construction du flocon de Koch.

L'ensemble triadique de Cantor

Cet ensemble a été étudié par le mathématicien allemand Georg Cantor (1845-1918).

Principe de construction :

- (i) E_0 est un segment de longueur 1.
- (ii) Pour obtenir E_{n+1} , on divise tous les segments de E_n en trois parties égales et on supprime la partie centrale.
- (iii) On continue ce processus à l'infini, i.e. $F = \lim_{n \rightarrow +\infty} E_n$.



La longueur de E_n est Ainsi, la longueur de F est

A l'étape n , il faut $N_{\epsilon_n}(E_n) = \dots\dots\dots$ boîtes de taille $\epsilon_n = \dots\dots\dots$ afin de recouvrir E_n . On a donc

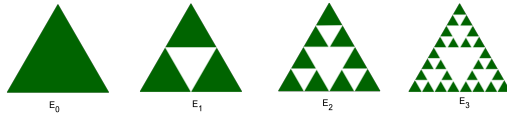
$$\dim_B(F) = \dots\dots\dots$$

Le triangle de Sierpiński

Cet objet fractal porte le nom du mathématicien polonais Waclaw Sierpiński (1882-1969). Dans la suite, on appellera “triangle plein” l’enveloppe convexe d’un triangle.

Principe de construction :

(i) T_1 est un triangle équilatéral plein de périmètre $P = 3$ et d’aire $A = \dots\dots\dots$



(ii) Pour obtenir T_{n+1} , on divise chaque triangle plein en quatre triangles semblables et on supprime le triangle central.

(iii) On continue ce processus à l’infini, i.e. $T = \lim_{n \rightarrow +\infty} T_n$.

Remarque 32. Dans la dernière figure, le triangle de Sierpiński est noir et les “trous” sont blancs.

Le périmètre de T_n est Ainsi, le périmètre de T est

L’aire de T_n est Ainsi, l’aire de T est

A l’étape n , il faut $N_{\epsilon_n}(T_n) = \dots\dots\dots$ boîtes de taille $\epsilon_n = \dots\dots\dots$ afin de recouvrir T_n . On a donc

$$\dim_B(T) = \dots\dots\dots$$

Le tapis de Sierpiński

Voici la version “carrée” du triangle de Sierpiński. On démarre avec un carré plein K_1 de côté 1, puis K_{n+1} est construit à partir de K_n en divisant chaque carré plein en 9 carrés semblables, puis en supprimant le carré central. On appelle $K := \lim_{n \rightarrow +\infty} K_n$.

L’aire de K_n est Ainsi, l’aire de K est

A l’étape n , il faut $N_{\epsilon_n}(K_n) = \dots\dots\dots$ boîtes de taille $\epsilon_n = \dots\dots\dots$ afin de recouvrir K_n . On a donc

$$\dim_B(K) = \dots\dots\dots$$

Remarque 33. Le tapis de Sierpiński peut aussi être vu comme l’une des faces de l’éponge de Menger (cf. Figure 1.14) décrite en 1926 par le mathématicien autrichien Karl Menger (1902-1985).

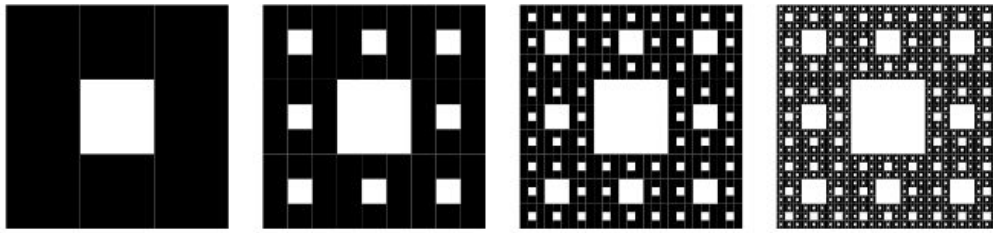


FIGURE 1.13 : Construction du tapis de Sierpiński

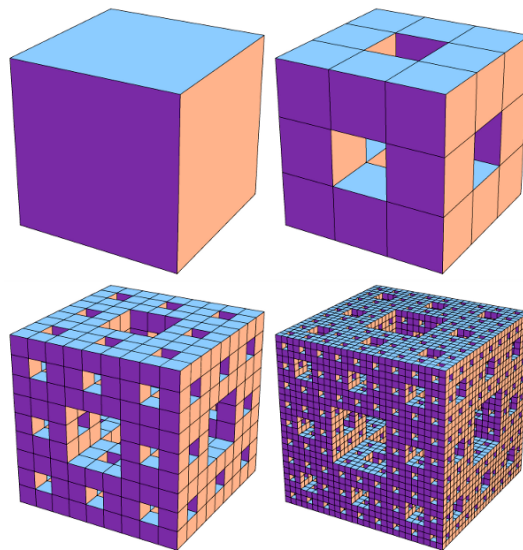


FIGURE 1.14 : Eponge de Menger

Intuitivement, l'aire de cet objet est

Intuitivement, le volume de cet objet est

La dimension de boîtes de cet objet est $\dim_B(E) = \frac{\log 20}{\log 3} \approx 2.727$.

Frontières d'un pays

Comme expliqué par Mandelbrot, Lewis Fry Richardson a mesuré la dimension fractale de la côte de la Grande-Bretagne et a trouvé

$$\dim_B(C) \approx 1.24.$$

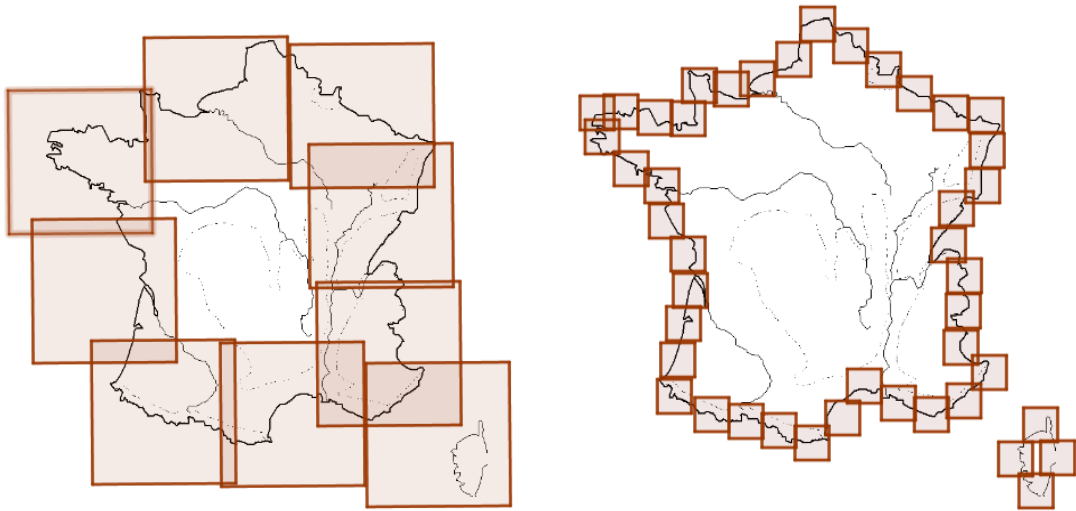


FIGURE 1.15 : Illustration du calcul de la dimension de boîtes pour les frontières de la France

Désavantage de la dimension de boîtes

Le problème avec \dim_B , c'est que l'on a la propriété suivante :

Proposition 34. Soit $F \subset \mathbb{R}^n$ un ensemble borné et \bar{F} sont adhérence. Si $\dim_B(F)$ et $\dim_B(\bar{F})$ existent, alors

$$\dim_B(F) = \dim_B(\bar{F}).$$

Démonstration. Soient K_1, \dots, K_k des cubes de côtés ϵ . Si l'ensemble fermé $\bigcup_{i=1}^k K_i \supset F$, alors Ainsi, on peut choisir $N_\epsilon(F) = N_\epsilon(\bar{F})$ et le résultat est démontré. □

Ainsi, si $F = \mathbb{Q} \cap [0, 1]$, alors $\dim_B(F) = \dim_B(\bar{F}) = \dots\dots\dots$
 La dimension de boîte ne sait pas faire la différence entre F et \bar{F} alors que F est , contrairement à \bar{F} .

1.2.3 Mesure et dimension de Hausdorff

Définition 35. Pour un sous-ensemble $U \subset \mathbb{R}^n$ non vide, on définit le diamètre de U , noté $|U|$, par

$$|U| := \sup\{\dots\dots\dots : x, y \in U\}.$$

Soit F un ensemble. Toute famille dénombrable $\{U_i\}$ telle que, pour tout i , $0 < |U_i| \leq \delta$, et $F \subset \bigcup_{i=1}^\infty U_i$ est appelée un δ -recouvrement de F .

Définition 36. Soit $F \subset \mathbb{R}^n$ et $s \geq 0$. Pour tout $\delta > 0$, on définit

$$\mathcal{H}_\delta^s(F) = \inf \left\{ \sum_{i=1}^{\infty} |U_i|^s : \{U_i\} \text{ et un } \delta\text{-recouvrement de } F \right\}.$$

La mesure de Hausdorff s -dimensionnelle de F est définie par

$$\mathcal{H}^s(F) := \dots\dots\dots$$

On admettra la proposition suivante :

Proposition 37. \mathcal{H}^s est une mesure borélienne.

Ainsi, on retrouve la fameuse propriété de changement d'échelle dont nous avons déjà parlé.

Proposition 38. Si $F \subset \mathbb{R}^n$ et $\lambda > 0$, alors $\mathcal{H}^s(\lambda F) = \dots\dots\dots$

Démonstration. On remarque tout d'abord la propriété suivante : si $\{U_i\}$ est un δ -recouvrement de F alors $\{\lambda U_i\}$ est un $\dots\dots\dots$ de λF . Ainsi, pour tout δ -recouvrement $\{U_i\}$ de F , on a

$$\mathcal{H}_{\lambda\delta}^s(\lambda F) \leq \dots\dots\dots = \lambda^s \sum_{i=1}^{\infty} |U_i|^s.$$

On en déduit donc que $\dots\dots\dots$, et ainsi

$$\mathcal{H}^s(\lambda F) = \lim_{\delta \rightarrow 0} \mathcal{H}_\delta^s(\lambda F) = \lim_{\delta \rightarrow 0} \mathcal{H}_{\lambda\delta}^s(\lambda F) \leq \lambda^s \lim_{\delta \rightarrow 0} \mathcal{H}_\delta^s(F) = \lambda^s \mathcal{H}^s(F).$$

Pour obtenir l'autre inégalité, on remplace λ par $\dots\dots\dots$ et F par $\dots\dots\dots$ □

Une autre propriété intéressante est la suivante :

Proposition 39. Soit $F \subset \mathbb{R}^n$ et $f : F \rightarrow \mathbb{R}^m$ une application α -höldérienne, c'est-à-dire qu'il existe $c > 0$ telle que pour tout $x, y \in F$,

$$|f(x) - f(y)| \leq c|x - y|^\alpha.$$

Alors, pour tout $s \geq 0$, on a $\mathcal{H}^{s/\alpha}(f(F)) \leq c^{s/\alpha} \mathcal{H}^s(F)$.

Démonstration. Soit $\{U_i\}$ un δ -recouvrement de F , alors on a $|f(F \cap U_i)| \leq \dots$ car f est α -höldérienne et ainsi la famille $\{f(F \cap U_i)\}$ est un ϵ -recouvrement de où $\epsilon = \dots$. On a donc

$$\sum_i |f(F \cap U_i)|^{s/\alpha} \leq \dots,$$

et en prenant sur les ϵ -recouvrements, on obtient

$$\dots \leq c^{s/\alpha} \sum_i |U_i|^s.$$

Donc, en prenant sur les δ -recouvrement, on obtient

$$\dots \leq \dots$$

Dès lors, quand $\delta \rightarrow 0$, on a $\epsilon \rightarrow 0$ et ainsi le résultat est démontré. □

Remarque 40. En particulier, quand $\alpha = 1$, on obtient que \mathcal{H}^s est invariante par

Proposition 41. Soit F un ensemble. Si $\mathcal{H}^s(F) < \infty$, alors $\mathcal{H}^t(F) = 0$ pour tout $t > s$.

Démonstration. Exercice. On pensera à écrire $|U_i|^t = |U_i|^s |U_i|^{t-s}$ et on montrera que $\mathcal{H}_\delta^t(F) \leq \delta^{t-s} \mathcal{H}_\delta^s(F)$. □

On a donc démontré que $\mathcal{H}^s(F)$ vaut d'abord l'infini pour s petit, puis zero quand s dépasse une certaine valeur critique. Il s'agit de la dimension de Hausdorff de F .

Définition 42. La dimension de Hausdorff d'un ensemble F est définie par

$$\dim_H(F) = \sup\{s : \mathcal{H}^s(F) = \infty\} = \inf\{s : \mathcal{H}^s(F) = 0\}.$$

Proposition 43. On a les propriétés suivantes :

- (i) \mathcal{H}^0 est
- (ii) \mathcal{H}^1 est
- (iii) Pour tout ensemble compact $F \subset \mathbb{R}^n$, $\mathcal{H}^s(F) = \dots$ si $s > n$.
- (iv) Si B est un borélien borné de \mathbb{R}^n avec $\mathcal{L}^n(B) > 0$, alors

$$\dim_H(B) = \dots$$

(v) Pour tout $F \subset \mathbb{R}^n$ borné ayant une dimension de boîte finie, on a

$$\dim_H(F) \leq \dim_B(F).$$

Démonstration. Admise. □

On peut montrer que $\dim_H(\mathbb{Q} \cap [0, 1]) = \dots\dots\dots$, et ainsi

$$\dots\dots\dots = \dim_H(\mathbb{Q} \cap [0, 1]) < \dim_B(\mathbb{Q} \cap [0, 1]) = 1.$$

En utilisant les bons δ -recouvrements, on peut montrer que les objets fractals étudiés précédemment ont les même dimensions de boîtes et de Hausdorff.

1.3 Autour de la formule d'Euler

Les résultats des deux premières sections de ce chapitre sont extraits de [2]. La dernière partie, sur les solides de Platon, est inspirée de [12].

1.3.1 Formule d'Euler et graphes planaires

Définition 44. Un graphe $G = (V, E)$ est la donnée de sommets V et d'arêtes E joignant ces points.

On dit qu'un graphe est planaire si on peut le représenter dans le plan \mathbb{R}^2 sans que ses arêtes ne se coupent. On décompose ainsi \mathbb{R}^2 en un nombre fini de régions connexes, incluant la région extérieure non bornée, qui sont appelées faces F .

On dit qu'un graphe est connexe si, pour tout couple de points $(x, y) \in V^2$, il existe une chaîne d'arêtes de E joignant x à y .

Un graphe est dit simple s'il ne contient ni boucle, ni double arête.

On notera $|V|$, $|E|$ et $|F|$ respectivement le nombre de sommets, d'arêtes et de faces de G .

Le degré d'un point est le nombre d'arêtes joignant ce point à d'autres points du graphe. Le degré d'une face est le nombre d'arêtes la bordant.

Théorème 45 (Euler). Si $G = (V, E)$ est un graphe planaire simple et connexe, alors

$$|V| - |E| + |F| = 2.$$

Démonstration. Soit T un arbre couvrant G minimal et sans circuit, ayant $|E_T|$ arêtes (c'est-à-dire non-orienté, acyclique et connexe). Alors $|V| = |E_T| + 1$. On définit le graphe dual G^* de G en définissant un sommet de G^* pour chaque face de G et une arête joignant les points quand les faces correspondantes de G sont adjacentes. Soit maintenant l'arbre T^* correspondant aux arêtes de $E \setminus E_T$. Alors T^* ne contient pas de circuit (sinon T ne serait pas connexe) et T^* est connexe et recouvre G^* . On a donc que $|F| = |E_{T^*}| + 1$. On en déduit donc que

$$|V| + |F| = |E_T| + |E_{T^*}| + 2 = |E| + 2.$$

□

Proposition 46. Soit $G = (V, E)$ un graphe planaire simple et connexe tel que $|E| \geq 2$, alors

$$2|E| = \sum_{f \in F} \deg(f) = \sum_{x \in V} \deg(x).$$

Démonstration. La première égalité découle du fait que chaque arête borde exactement 2 faces, et ainsi la somme des degrés des faces est égale à deux fois le nombre

d'arêtes. La deuxième égalité vient du fait que $\deg(x)$ est égal au nombre d'arêtes issues de x et que chaque arête possède deux sommets. \square

Proposition 47. Soit $G = (V, E)$ un graphe planaire simple et connexe, alors :

- (i) on a $|E| \leq 3|V| - 6$,
- (ii) si G est sans triangle, alors $|E| \leq 2|V| - 4$.

Démonstration. Chaque face de G est bordée par au moins 3 arêtes, i.e. pour tout $f \in F$, $\deg(f) \geq 3$. On a donc, d'après la proposition précédente,

$$2|E| = \sum_{f \in F} \deg(f) \geq 3|F|.$$

D'après la formule d'Euler, on a donc

$$2|E| \geq 3(2 + |E| - |V|),$$

c'est-à-dire $|E| \leq 3|V| - 6$. La deuxième partie de la proposition se montre de la même manière. Chaque face étant bordé par au moins 4 arêtes, on obtient $2|E| \geq 4|F|$ et on conclut de même avec la formule d'Euler. \square

1.3.2 Théorème de Pick

Proposition 48. Pour toute base (e_1, e_2) de \mathbb{Z}^2 , on a $\text{Aire}(e_1, e_2) = 1$.

Démonstration. On remarque tout d'abord que $\text{Aire}((1, 0), (0, 1)) = 1$. Notons maintenant $e_1 = (a, b)$ et $e_2 = (c, d)$ une autre base de \mathbb{Z}^2 . On sait qu'il existe $Q \in GL_n(\mathbb{Z})$ tel que $\text{Mat}(e_1, e_2) = \text{Mat}((1, 0), (0, 1))Q$. On sait que $\det Q \in \mathbb{Z}$ et que $QQ^{-1} = I_2$, donc nécessairement $|\det Q| = 1$. On en déduit donc que $\text{Aire}(e_1, e_2) = 1$. \square

Proposition 49. Tout triangle élémentaire $\Delta = \text{conv}(p_0, p_1, p_2)$, c'est-à-dire dont les sommets sont dans \mathbb{Z}^2 et que son enveloppe convexe ne contient aucun autre point du réseau, a pour aire $1/2$.

Démonstration. Le parallélogramme $P = \{p_0, p_1, p_2, p_1 + p_2 - p_0\}$ ainsi que \mathbb{Z}^2 sont invariant par la symétrie centrale, de centre le milieu de $[p_1, p_2]$, définie par

$$\sigma : x \mapsto p_1 + p_2 - x.$$

Ainsi, $P = \Delta \cup \sigma(\Delta)$ est un polygone élémentaire et ses translats entiers recouvrent le plan. On en déduit que $(p_1 - p_0, p_2 - p_0)$ est une base de \mathbb{Z}^2 et donc que $\text{Aire}(p_1 - p_0, p_2 - p_0) = 1$. On a ainsi que $\text{Aire}(\text{conv}(p_0, p_1, p_2)) = 1/2$. \square

Théorème 50 (Théorème de Pick). L'aire de tout polygone $Q \subset \mathbb{R}^2$ dont les sommets appartiennent à \mathbb{Z}^2 vérifie

$$\text{Aire}(Q) = n_i + \frac{n_b}{2} - 1,$$

où n_i (respectivement n_b) désigne le nombre de points entiers à l'intérieur (respectivement sur le bord) de Q .

Démonstration. On admet que Q peut être triangulé en utilisant tous les n_i points du réseau intérieur à Q ainsi que tous les n_b sur le bord de Q . Cette triangulation donne un graphe planaire connexe et simple. De plus, il partage le plan en une face non-bornée et $|F| - 1$ triangles d'aire $1/2$, d'après la proposition précédente. On a donc

$$\text{Aire}(Q) = \frac{|F| - 1}{2}.$$

Chaque triangle est bordé par trois arêtes, et :

- chacune des e_i arêtes intérieures borde 2 triangles,
- chacune des e_b arêtes du bord borde 1 triangle.

Ceci implique que

$$3(|F| - 1) = 2e_i + e_b \iff |F| = 2(|E| - |F|) - e_b + 3.$$

De plus, on a $e_b = n_b$, et donc, d'après la formule d'Euler, on obtient

$$|F| = 2(|E| - |F|) - e_b + 3 = 2(|V| - 2) - n_b + 3 = 2n_i + n_b - 1.$$

On a donc

$$\text{Aire}(Q) = \frac{2n_i + n_b - 1 - 1}{2} = n_i + \frac{n_b}{2} - 1.$$

□

1.3.3 Polyèdres réguliers et pavages de la sphère

Une deuxième application de la formule d'Euler à un polyèdre (ce qui est possible par projection stéréographique du polyèdre dans le plan) est la suivante :

Proposition 51. Tout polyèdre (tel que chaque sommet appartient à trois polygones) composé seulement de pentagones et d'hexagones a exactement 12 pentagones.

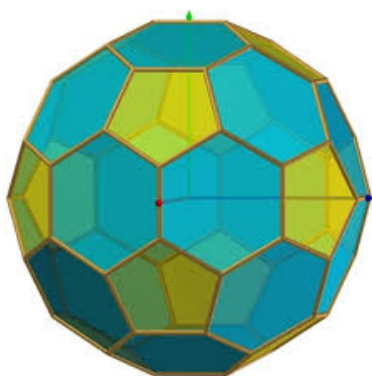
Démonstration. Soit P le nombre de pentagone et H le nombre d'hexagones. Alors le nombre total de faces du polyèdre est

$$|F| = P + H.$$

Comme chaque sommet appartient à trois polygones (admis), et chaque arête appartient à deux polygones, on obtient

$$|V| = \frac{5P + 6H}{3}, \quad |E| = \frac{5P + 6H}{2}.$$

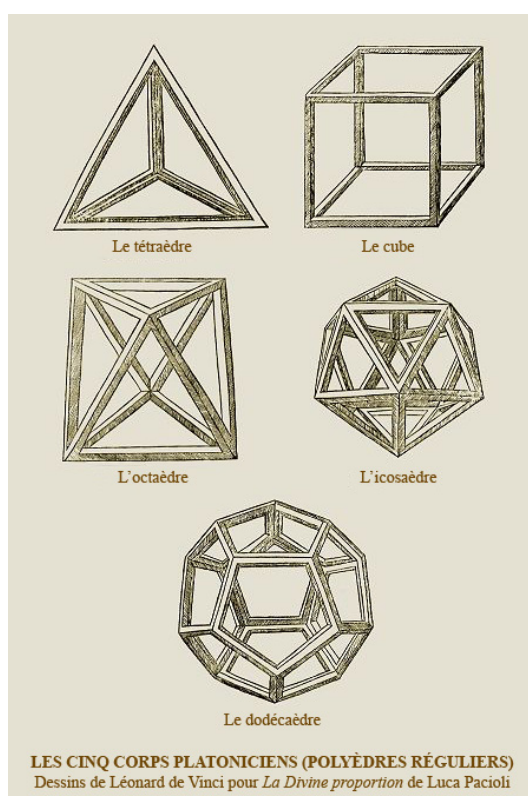
On calcule ainsi que $|V| - |E| + |F| = \frac{P}{6}$, et ainsi d'après la formule d'Euler, on obtient que $P = 12$. \square



Définition 52. Un solide est régulier si et seulement si toutes ses faces sont identiques à un même polygone régulier et le même nombre de faces se rencontrent à chacun de ses sommets.

Théorème 53. Il n'existe que 5 solides réguliers, appelés solides de Platon :

- le tétraèdre (4 sommets, 4 faces, 6 arêtes),
- le cube (8 sommets, 6 faces, 12 arêtes),
- l'octaèdre (6 sommets, 8 faces, 12 arêtes),
- le dodécaèdre (20 sommets, 12 faces, 30 arêtes),
- l'icosaèdre (12 sommets, 20 faces, 30 arêtes).



Démonstration. Soit S un polyèdre régulier ayant n sommets, a arêtes et f faces, possédant $k \geq 3$ arêtes par faces et $d \geq 3$ arêtes se rencontrant à chaque sommet. On a :

(i) comme chaque arête appartient à deux faces, $kf = 2a$,

(ii) comme chaque arête possède deux sommets, $dn = 2a$.

La formule d'Euler s'applique à tout polyèdre, c'est-à-dire que l'on a

$$n - a + f = 2.$$

On remplace n et f par $2a/d$ et $2a/k$ et on obtient

$$\frac{2a}{d} - a + \frac{2a}{k} = 2.$$

On divise l'équation par $2a$ et on obtient

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{a} + \frac{1}{2}.$$

Nous allons montrer que cette équation n'admet que 5 solutions entières. Celle-ci implique que $\frac{1}{k} + \frac{1}{d} > \frac{1}{2}$.

Cas 1 : Si $d \geq 6$, alors comme on a $k \geq 3$ et que $k \mapsto \frac{1}{k}$ est décroissante, il suffit de regarder le cas $k = 3$. Comme $\frac{1}{6} + \frac{1}{3} \leq \frac{1}{2}$, l'équation n'admet pas de solution.

Cas 2 : Si $d = 5$. Alors pour $k = 3$, l'équation a une solution si $a = 30$ (Icosaèdre). Mais si $k \geq 4$, alors $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ et l'équation n'admet pas de solution.

Cas 3 : Si $d = 4$, alors pour $k = 3$, l'équation a une solution $a = 12$ (Octaèdre), et si $k \geq 4$, alors $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ et l'équation n'admet pas de solution.

Cas 4 : Si $d = 3$, alors

- pour $k = 3$, on aura $a = 6$ (Tétraèdre),
- pour $k = 4$, on aura $a = 12$ (Cube),
- pour $k = 5$, on aura $a = 30$ (Dodecaèdre).

Par contre, pour $k \geq 6$, $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ et l'équation n'admet pas de solution.

□

1.4 Topologie sur les espaces matriciels

Dans cette partie (que l'on peut retrouver en tant qu'exercice dans [16]), nous allons démontrer plusieurs résultats portant sur les sous-ensembles de $M_n(\mathbb{R})$ ou $M_n(\mathbb{C})$.

Proposition 54. L'ensemble des matrices inversibles $GL_n(\mathbb{R})$ est un ouvert dense dans $M_n(\mathbb{R})$. De plus $M_n(\mathbb{R}) \setminus GL_n(\mathbb{R})$ est fermé mais non compact, si $n \geq 2$.

Démonstration. Montrons que $GL_n(\mathbb{R})$ est un ouvert de $M_n(\mathbb{R})$. Soit $\det : M \mapsto \det(M)$ de $M_n(\mathbb{R})$ dans \mathbb{R} . Alors $\det(M)$ est une fonction polynomiale des coefficients de M , donc \det est continue sur $M_n(\mathbb{R})$. De plus, $GL_n(\mathbb{R}) = \det^{-1}(\mathbb{R}^*)$ et \mathbb{R}^* est un ouvert de \mathbb{R} . Ainsi, $GL_n(\mathbb{R})$ est l'image réciproque d'un ouvert par une application continue, donc $GL_n(\mathbb{R})$ est un ouvert de $M_n(\mathbb{R})$.

Montrons que $GL_n(\mathbb{R})$ est dense dans $M_n(\mathbb{R})$. Soit $A \in M_n(\mathbb{R})$, alors le polynôme caractéristique de A , noté χ_A , n'admet qu'un nombre fini de racines. Il existe donc x_0 tel que, pour tout $0 < x < x_0$, $\chi_A(x) \neq 0$. On en déduit donc qu'il existe $p_0 \in \mathbb{N}$ tel que pour tout entier $p \geq p_0$, $\det\left(A - \frac{1}{p}I_n\right) \neq 0$. Pour tout $p \geq p_0$, soit $A_p := A - \frac{1}{p}I_n$. Alors pour chaque $p \geq p_0$, $A_p \in GL_n(\mathbb{R})$ et $\lim_{p \rightarrow +\infty} A_p = A$ (pour n'importe quelle norme sur $M_n(\mathbb{R})$). Ainsi, on a trouvé une suite de matrices inversibles qui tend vers A , et donc $GL_n(\mathbb{R})$ est dense dans $M_n(\mathbb{R})$.

Comme $GL_n(\mathbb{R})$ est ouvert dans $M_n(\mathbb{R})$, $M_n(\mathbb{R}) \setminus GL_n(\mathbb{R})$ est donc fermé. Montrons que cet ensemble n'est pas borné. Il suffit de définir $A_n = nE_{1,1}$, où $E_{1,1}$ a uniquement son coefficient $e_{1,1} = 1$ et tous les autres sont égaux à 0. Cette suite $(A_n)_n$ n'est pas bornée et, pour tout $n \in \mathbb{N}$, $A_n \in M_n(\mathbb{R}) \setminus GL_n(\mathbb{R})$. \square

Proposition 55. L'espace des matrices orthogonales $O_n(\mathbb{R})$ est compact et non-convexe.

Démonstration. On définit $f : M \mapsto MM^t$. L'application f est continue comme composée d'applications continues. De plus $O_n(\mathbb{R}) = f^{-1}(\{I_n\})$ et $\{I_n\}$ est un fermé de $M_n(\mathbb{R})$. Ainsi, $O_n(\mathbb{R})$ est un fermé comme image réciproque d'un fermé par une application continue. Montrons maintenant que $O_n(\mathbb{R})$ est borné. On utilise le fait qu'une matrice est orthogonale si et seulement si ses colonnes forment une base orthonormée de \mathbb{R}^n . Ainsi, pour tout $A \in O_n(\mathbb{R})$, $\|A\| \leq C$, où C est une constante indépendante de A , ce qui implique que $O_n(\mathbb{R})$ est borné.

Pour montrer que $O_n(\mathbb{R})$ n'est pas convexe, on utilise le contre-exemple suivant : $\frac{I_n}{2} - \frac{I_n}{2} = 0 \notin O_n(\mathbb{R})$, alors que I_n et $-I_n$ appartiennent à $O_n(\mathbb{R})$. \square

Proposition 56. L'espace $S_n(\mathbb{R})$ des matrices symétriques réelles est un fermé de $M_n(\mathbb{R})$.

Démonstration. Comme $S_n(\mathbb{R})$ est un sous-espace vectoriel de dimension finie de $M_n(\mathbb{R})$, alors il est fermé. \square

Proposition 57. Soit $p \in \{0, 1, \dots, n\}$. L'ensemble des matrices de rang inférieur ou égal à p est un fermé de $M_n(\mathbb{R})$.

Démonstration. On remarque tout d'abord que si $p \in \{0, n\}$, alors le résultat est évident. Soit maintenant $p \in \{1, \dots, n-1\}$ et $A \in M_n(\mathbb{R})$. On a que $\text{rang}(A) \leq p$ si et seulement si tous les mineurs de A de taille $p+1$ sont nuls. Soient $I, J \subset \{1, \dots, n\}$, chacun de cardinal $p+1$ et $A_{I,J}$ la matrice extraite de A , de format $p+1$, dont les numéros de lignes sont dans I et les numéros de colonnes sont dans J . L'application $A \mapsto A_{I,J}$ est continue, et, par continuité du déterminant, $f_{I,J} : A \mapsto \det(A_{I,J})$ est continue sur $M_n(\mathbb{R})$. On a donc que $f_{I,J}^{-1}(\{0\}) = \{A; \det(A_{I,J}) = 0\}$ est un fermé de $M_n(\mathbb{R})$ comme image réciproque d'un fermé par une application continue. Ainsi, l'ensemble des matrices de rang plus petit ou égal à p est un fermé comme intersection d'ensembles fermés. \square

Proposition 58. L'ensemble des matrices diagonalisables dans $M_n(\mathbb{C})$ est dense dans $M_n(\mathbb{C})$. Ce n'est pas le cas si on remplace \mathbb{C} par \mathbb{R} .

Démonstration. Soit $A \in M_n(\mathbb{C})$ et $sp(A) = (\lambda_i)_{1 \leq i \leq n}$ l'ensemble des racines du polynôme caractéristique de A . On sait que A est triangularisable (ou trigonalisable), c'est-à-dire qu'il existe une matrice $P \in GL_n(\mathbb{C})$ et T triangulaire avec $t_{i,i} = \lambda_i$ pour tout $1 \leq i \leq n$ telles que $A = PTP^{-1}$. On munit $M_n(\mathbb{C})$ d'une norme sous-multiplicative ($\forall A, B, \|AB\| \leq \|A\|\|B\|$) et on sait donc, par équivalence des normes dans $M_n(\mathbb{C})$ de dimension finie, qu'il existe $K > 0$ tel que $\|M\| \leq K\|M\|_\infty$.

Soit $\varepsilon > 0$, alors il existe $(\varepsilon_1, \dots, \varepsilon_n)$ tels que, pour tout $1 \leq k \leq n$,

$$0 \leq \varepsilon_k < \frac{\varepsilon}{K\|P\|\|P^{-1}\|},$$

et les $\varepsilon_k + \lambda_k$ sont deux-à-deux distincts. Il suffit de choisir $\varepsilon_1 = 0$, puis $\varepsilon_2 \in [0, \varepsilon K^{-1}\|P\|^{-1}\|P^{-1}\|^{-1})$ tel que $\lambda_2 + \varepsilon_2 \neq \lambda_1 + \varepsilon_1$, etc. On pose $D = \text{diag}(\varepsilon_1, \dots, \varepsilon_n)$, $T' = T + D$ et $A' = PT'P^{-1}$. Ainsi, les valeurs propres de A' sont les $\lambda_k + \varepsilon_k$ et elles sont donc deux-à-deux distinctes. On en déduit que A' est diagonalisable et que

$$\|A - A'\| = \|PDP^{-1}\| \leq \|P\|\|D\|\|P^{-1}\| \leq K\|P\|\|P^{-1}\|\|D\|_\infty < \varepsilon.$$

On a donc montré que pour tout $A \in M_n(\mathbb{C})$ et pour tout $\varepsilon > 0$, il existe une matrice A' diagonalisable telle que $\|A - A'\| < \varepsilon$, ce qui démontre le résultat.

On ne peut pas remplacer \mathbb{C} par \mathbb{R} . Il suffit de choisir

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad E = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

où $\|E\|_\infty \leq 1/4$. On montre facilement que le discriminant de χ_{A+E} est négatif. Ainsi, on a construit une boule fermée centrée en A de matrices réelles qui ne sont pas diagonalisables. \square

Proposition 59. L'ensemble des matrices diagonalisables de $M_n(\mathbb{R})$ est connexe par arcs.

Démonstration. Soient A, B diagonalisables. On définit les trois chemins suivants, tous de $[0, 1]$ dans $M_n(\mathbb{R})$: $\gamma_1(t) = (1-t)A$, $\gamma_2(t) = tB$ et $\gamma(t) = \gamma_1(2t)$ si $t \in [0, 1/2]$, $\gamma(t) = \gamma_2(2t-1)$ si $t \in [1/2, 1]$. On remarque que γ_1 (respectivement γ_2) est un chemin continue qui joint A à la matrice nulle (respectivement la matrice nulle à B). Ainsi, γ est un chemin continue joignant A à B . De plus, pour tout $t \in [0, 1]$, $(1-t)A$ et tB sont diagonalisables. En effet, si M est diagonalisable, alors il existe une matrice inversible P et une matrice diagonale D telles que $M = PDP^{-1}$, et ainsi, pour tout $\lambda \neq 0$, $\lambda M = P(\lambda D)P^{-1}$, c'est-à-dire que λM est aussi diagonalisable. On a donc construit un chemin γ de matrices diagonalisables qui joint A à B , donc le résultat est démontré. \square

1.5 Calculs d'intégrales

Le but de ce chapitre est de rappeler, ou de découvrir, quelques “trucs” pour calculer des intégrales. L'intégralité de cette partie se fera sous forme d'exercices. On peut les retrouver dans [18] et [13].

1.5.1 Intégrale gaussienne

Exercice 60. Montrer que $\int_{\mathbb{R}} e^{-ax^2} dx = \sqrt{\frac{\pi}{a}}$.

1.5.2 Parité

Exercice 61. Calculer $I = \int_{-1}^1 \frac{x^3 - 2 \sin(x)}{\sqrt{1+x^4}} dx$.

1.5.3 Transformations utiles

Les deux transformations suivantes peuvent être utiles (sous réserve de pouvoir les faire) :

$$\int_a^b f(x) dx = \frac{1}{2} \int_a^b f(x) + f(a+b-x) dx,$$

$$\int_0^{\infty} f(x) dx = \frac{1}{2} \int_0^{\infty} f(x) + \frac{f\left(\frac{1}{x}\right)}{x^2} dx.$$

Exercice 62. Calculer les deux intégrales suivantes :

$$I_1 = \int_3^7 \frac{\ln(x+2)}{\ln(24+10x-x^2)} dx, \quad I_2 = \int_0^{+\infty} \frac{\ln(2x)}{1+x^2} dx.$$

1.5.4 Intégration par parties

Exercice 63. Calculer les intégrales suivantes :

$$I = \int_1^7 \ln(1+x) dx$$

$$B(m, n) = \int_0^1 x^m (1-x)^n dx, \quad m, n \in \mathbb{N}, \quad (\text{fonction bêta})$$

$$W_n = \int_0^{\frac{\pi}{2}} \sin^n x dx, \quad n \in \mathbb{N}, \quad (\text{Intégrale de Wallis})$$

1.5.5 Substitution de Weierstrass

Exercice 64. Calculer $I = \int_0^{\frac{\pi}{2}} \frac{dx}{2 + \cos x}$.

1.5.6 Utilisation du développement en série entière

Exercice 65. Calculer $I = \int_0^1 \ln(x) \ln(x-1) dx$.

1.5.7 Intersion d'intégrales

Exercice 66. Après avoir calculé $\int_0^a x^y dy$, déterminer la valeur de l'intégrale

$$I(a) = \int_0^1 \frac{x^a - 1}{\ln(x)} dx.$$

1.5.8 Changement d'échelle

Soit $f(R) = \int_{C_R} \int_{C_R} \frac{dx dy}{|x-y|}$, où $C_R = \{x \in \mathbb{R}^d; \frac{R}{2} \leq |x| \leq R\}$. Montrer, en calculant $f(\lambda R)$ pour $\lambda > 0$, que l'on a

$$f(R) = f(1)R^{2d-1}.$$

1.5.9 Fonctions harmoniques

On dit qu'une fonction est harmonique sur \mathbb{R}^2 si $\Delta f(x, y) = 0$ pour tout $(x, y) \in \mathbb{R}^2$. En particulier, on a la propriété suivante :

Proposition 67. Si f est harmonique sur \mathbb{R}^2 , alors

$$\int_0^{2\pi} f(a + r \cos \theta, b + r \sin \theta) d\theta = 2\pi f(a, b).$$

Exercice 68. Calculer $\int_0^{2\pi} e^{\cos x} \cos(\sin x) dx$.

1.5.10 Le “truc” favori de Feynmann

L'idée suivante a été utilisée de nombreuses fois par le physicien Richard Feynmann. Soit

$$I(t) := \int_{a(t)}^{b(t)} f(x, t) dx,$$

alors on a

$$I'(t) = \int_{a(t)}^{b(t)} \frac{\partial f}{\partial t}(x, t) dx + b'(t)f(b(t), t) - a'(t)f(a(t), t).$$

L'idée est que l'on peut rajouter un paramètre et dériver les égalités en fonction de ce paramètre.

Exercice 69. On rappelle que $\int_0^\infty \frac{dx}{x^2 + a^2} = \frac{\pi}{2a}$. Montrer que l'on a

$$(i) \int_0^\infty \frac{dx}{(x^2 + a^2)^2} = \frac{\pi}{4a^3},$$

$$(ii) \int_0^\infty \frac{dx}{(x^2 + a^2)^3} = \frac{3\pi}{16a^5}.$$

Exercice 70. On rappelle que $\int_{\mathbb{R}} e^{-\frac{x^2}{2}} dx = \sqrt{2\pi}$. Le but de cet exercice est de calculer

$$I(t) = \int_0^\infty \cos(tx) e^{-\frac{x^2}{2}} dx$$

en fonction de t .

(i) Montrer, à l'aide d'une intégration par parties, que $I'(t) = -tI(t)$.

(ii) Conclure.

Exercice 71 (Intégrale discontinue de Dirichlet). Soit, pour tout $t > 0$ et $a \in \mathbb{R}$,

$$g(t) = \int_0^\infty e^{-tx} \frac{\sin(ax)}{x} dx.$$

(i) Montrer que $g'(t) = -\frac{a}{a^2 + t^2}$.

(ii) En déduire que $\int_0^\infty \frac{\sin ax}{x} dx = \operatorname{sgn}(a) \frac{\pi}{2}$ si $a \neq 0$, et 0 sinon.

Exercice 72. Utiliser la méthode précédente pour montrer que, pour tout $a, b \in (0, \infty)$,

$$I(a, b) := \int_0^\infty \frac{\arctan(ax) - \arctan(bx)}{x} dx = \frac{\pi}{2} \ln \left(\frac{a}{b} \right),$$

et pour tout $a > 0$,

$$I(a) := \int_0^\infty \frac{e^{-5x} - e^{-ax}}{x} dx = \ln \left(\frac{a}{5} \right).$$

1.6 Notations

Il y a de nombreuses différences de notations entre le Français et l'Anglais. Le but de cette partie est de lister les principales.

1. **Nombres.** En Français, le séparateur décimal est une virgule (,) alors que c'est un point (.) en Anglais.

$$\underset{\text{Anglais}}{1,345.67} = \underset{\text{Français}}{1345,67}$$

2. **Nombres positifs et négatifs.** En Français, les nombres positifs (respectivement négatifs) sont ceux qui sont supérieurs ou égaux (respectivement inférieurs ou égaux) à zéro. Pour exclure 0, on parle de nombres strictement positifs ou strictement négatifs.

$$\underset{\text{Anglais}}{\text{Positive}} = \underset{\text{Français}}{\text{Strictement positif}}, \quad \underset{\text{Anglais}}{\text{Non-negative}} = \underset{\text{Français}}{\text{Positif}}$$

3. **Coordonnées et vecteurs.** En Français, le point-virgule (;) est parfois utilisé à la place de la virgule pour lister les coordonnées d'un vecteur ou d'un point. C'est tout simplement pour éviter toute confusion en cas de nombres décimaux.

$$\underset{\text{Anglais}}{(1.2, 2.5, 8.1)} = \underset{\text{Français}}{(1, 2; 2, 5; 8, 1)}$$

4. **Intervalles.** En Français, les crochets ([]) sont utilisés à la place des parenthèses pour noter les intervalles.

$$\underset{\text{Anglais}}{[a, +\infty)} = \underset{\text{Français}}{[a, +\infty[} \quad \underset{\text{Anglais}}{(-\infty, +\infty)} = \underset{\text{Français}}{]-\infty, +\infty]}$$

5. **Nombres entiers naturels.** En Français, 0 est inclu dans l'ensemble des nombres entiers naturels.

$$\underset{\text{Anglais}}{\mathbb{N}} := \{1, 2, \dots\}; \quad \underset{\text{Français}}{\mathbb{N}} := \{0, 1, 2, \dots\}$$

Pour enlever 0, on utilise simplement l'étoile : \mathbb{N}^* .

6. **Intervalles d'entiers.** En Français, il existe une notation utilisant les crochets \llbracket et \rrbracket .

$$\{4, 5, 6, \dots, 10\} = \llbracket 4, 10 \rrbracket$$

Anglais Français

7. **Produit vectoriel.** En Français, le produit vectoriel (“cross product” en Anglais) est noté en utilisant \wedge plutôt que \times .

$$\vec{u} \times \vec{v} = \vec{u} \wedge \vec{v}$$

Anglais Français

8. **Fonction hyperboliques.** Voici les noms en Français et en Anglais des fonctions hyperboliques.

$$\cosh = ch, \quad \sinh = sh, \quad \tanh = th,$$

Anglais Français Anglais Français Anglais Français

$$\operatorname{arcosh} = \operatorname{argch}, \quad \operatorname{arcsinh} = \operatorname{argsh}, \quad \operatorname{artanh} = \operatorname{argth}$$

Anglais Français Anglais Français Anglais Français

9. **Matrice transposée.** En Français, le symbole t est utilisé à gauche de la matrice.

$$M^\top = {}^tM$$

Anglais Français

10. **Calcul d’une intégrale.** En Français, on utilise des crochets pour le calcul d’une intégrale.

$$\int_1^2 x dx = \left. \frac{1}{2} x^2 \right|_1^2, \quad \int_1^2 x dx = \left[\frac{1}{2} x^2 \right]_1^2$$

Anglais Français

11. **Coefficient binomial.** En Français, on peut parfois trouver la notation C_n^k pour le coefficient binomial (i.e. le nombre de combinaisons à k éléments dans un ensemble à n éléments).

$$\binom{n}{k} = C_n^k$$

Anglais Français

1.7 Vocabulaire

| Français | Anglais |
|--------------------------|---------------------|
| on a | we have |
| comme on a | since we have |
| ainsi | thus |
| appartenir à | to belong to |
| appartient à | belongs to |
| au moins | at least |
| au plus | at most |
| compris entre x et y | between x and y |
| déduire | deduce |
| on en déduit | we deduce from that |
| définir | to define |
| défini(e) | defined |
| dénombrable | countable |
| donc | therefore |
| entier | integer |
| écrire | write |
| on écrit | we write |
| un ensemble | a set |
| au hasard | randomly |
| il existe | there exists |
| impliquer | to imply |
| ce qui implique | which implies |
| inférieur à | smaller than |
| milieu | midpoint |
| montrer | to show |
| montrons que | let us show that |
| puissance | exponent |
| x au carré | x^2 |
| x au cube | x^3 |
| x à la puissance d | x^d |

| Français | Anglais |
|------------------------------------|-----------------------------------|
| on obtient | we obtain |
| par | by |
| parité | parity |
| pair | even |
| impair | odd |
| plus grand que | larger than |
| strictement | strictly |
| pour tout | for all |
| prouver | to prove |
| prouvons que | let us prove that |
| que | that |
| restreindre | to restrict |
| on restreint | we restrict |
| résultat | result |
| racine de a | \sqrt{a} |
| nombre rationnel | rational number |
| l'ensemble des réels | the real numbers |
| un réel x | a real number x |
| \mathbb{R} privé de \mathbb{Q} | $\mathbb{R} \setminus \mathbb{Q}$ |
| si..., alors.... | If... then.... |
| soit | Let |
| on souhaite | we wish |
| si et seulement si | if and only if |
| supérieur à | larger than |
| supposer | to assume |
| on suppose | we assume |
| tel(s) que | such that |
| tendre | to tend |
| x tend vers 0 | x tends to 0 |
| toujours | always |

Bibliographie

- [1] Actualitix, *Carte de la Bretagne*. <https://www.actualitix.com/carte-bretagne.html>.
- [2] Aigner, M. and Ziegler, G. M. *Raisonnements divins*, Springer Verlag France, 2013.
- [3] Bankov, K., *Applications of the Pigeon-Hole Principle*, The Mathematical Gazette 79 (485), pp. 286–292, 1995.
- [4] Bova, C. et Di Filippo, C. et Gigliotti, P. et Alfieri, A., *Cathedrals, houses and blue poles* Presentation. Liceo Scientifico L. Siciliani Catanzaro Fractals and art European Student Conference in Mathematics EUROMATH, 2012.
- [5] Derksen, H., *Problem set 7 : pigeon hole principle*, <http://www.math.lsa.umich.edu/~hderksen/ProblemSolving/PS7.pdf>.
- [6] Falconer, K., *Fractal Geometry : Mathematical Foundations and Applications*. Wiley-Blackwell, 2003.
- [7] Mandelbrot, B., *How long is the coast of Britain? Statistical self-similarity and fractional dimension*, Science 156 (3775), pp. 636–638, 1967.
- [8] Meyer, B., *Graphes, formule d'Euler et solides de Platon*. http://paestel.fr/sites/default/files/Mat_les_ressources/Terminale/Atelier.
- [9] Nahin, P. J., *Inside Interesting Integrals*, Undergraduate Lecture Notes in Physics, Springer, New York, NY, 2014.
- [10] Niven, I., *Irrational Numbers*, Carus Mathematical Monographs (Book 11), The Mathematical Association of America, 2005.
- [11] Rouget, J.-L., *Exo 7 Topologie*, <http://exo7.emath.fr/ficpdf/fic00134.pdf>.
- [12] Riter, P., *Petit recueil d'énigmes*, http://www.univ-orleans.fr/mapmo/membres/cordier/centre-galois/doc/ENIGMES_AVEC_SOL.pdf.
- [13] RRL, *An application of the pigeonhole principle in analysis*, <https://math.stackexchange.com/questions/2282584/an-application-of-the-pigeonhole-principle-in-analysis/2282655>.
- [14] Trevor, B. et Shenoy, V. et Gaba, P. et al., *Integration Tricks*, <https://brilliant.org/wiki/integration-tricks/>.

- [15] Wikipedia, *Hall's marriage theorem*, <https://en.wikipedia.org/wiki/Hall>.

Capítulo 2

ToMaTS Español

2.1 El principio del palomar

En este capítulo estudiaremos el principio del palomar. Empezaremos con el enunciado formal y posteriormente trabajaremos algunas de sus aplicaciones en relación con otros resultados clásicos en matemáticas.

2.1.1 ¿Qué es el principio del palomar?

El principio del palomar es un resultado que permite descartar la existencia de una función inyectiva entre dos conjuntos finitos. Este resultado no tiene hipótesis adicionales sobre la función, o sobre alguna estructura adicional de los conjuntos, simplemente depende del cardinal del dominio y codominio de la función. El cardinal de un conjunto X será denotado como $|X|$.

Teorema 73 (Principio del palomar). Sean X y Y dos conjuntos finitos. Si f es una función de X en Y y $|X| > |Y|$, entonces existen $x_1, x_2 \in X$ con $x_1 \neq x_2$ tales que $f(x_1) = f(x_2)$.

Intuitivamente esto significa que una función entre dos conjuntos finitos en la que el cardinal del dominio es mayor al cardinal del codominio, no puede ser inyectiva. Es importante resaltar que el principio del palomar solo garantiza la existencia de dos elementos con la misma imagen, sin embargo no indica cómo encontrarlos y tampoco da información sobre el valor de la imagen.

Ejemplos

Veamos algunos ejemplos del uso del principio del palomar

- (i) Suponga que se dibujan 5 puntos en el interior de un triángulo equilátero cuyo lado mide 2 metros. Demuestre que al menos dos de los puntos están a una distancia menor o igual a 1 metro.

Demostración. En la parte izquierda de la Figura 2.1 tenemos un triángulo equilátero de lado 2 con 5 puntos en su interior. Para probar que dos de estos puntos están a una distancia menor o igual a 1 dibujamos el triángulo formado por los puntos medios de cada lado del triángulo original (ilustrado en la parte central de la Figura 2.1). El triángulo interior divide al triángulo original en cuatro triángulos equiláteros de lado 1.

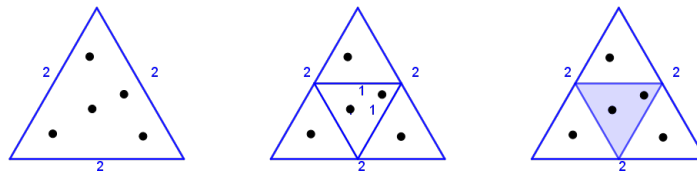


Figura 2.1: Triángulo de lado 2 con cinco puntos en su interior y existencia de dos puntos que están a una distancia menor a uno entre ellos.

Ahora consideramos el conjunto X formado los 5 puntos dentro del triángulo y el conjunto Y formado por los cuatro triángulos de lado 1, y definimos f como la función que a cada punto le asigna el triángulo en el cual yace. En este caso $|X| = 5 > 4 = |Y|$, entonces por el principio del palomar tenemos que esta función no es inyectiva, es decir, hay al menos dos puntos que están ubicados en el mismo triángulo pequeño. En la Figura 2.1 esto sucede en el triángulo central. Dado que la longitud del lado de cada triángulo pequeño es 1 metro, la distancia entre estos dos puntos es menor o igual a un metro. \square

- (ii) Sean x_1, x_2, x_3, x_4, x_5 puntos en \mathbb{Z}^2 y suponga que se dibuja el grafo completo generado por estos puntos (es decir, se dibujan todas las líneas posibles uniendo los puntos). Demuestre que al menos una arista del grafo intersecta $\mathbb{Z}^2 - \{x_1, x_2, \dots, x_5\}$.

Demostración. Si (a, b) y (c, d) son dos puntos en el plano, entonces el punto medio del segmento que los une está dado por $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$. Para probar el enunciado mostraremos que el punto medio de uno de los segmentos en el grafo está en $\mathbb{Z}^2 - \{x_1, x_2, \dots, x_5\}$.

Si $(a, b), (c, d) \in \mathbb{Z}^2$ entonces el punto medio $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$ tiene coordenadas enteras si $a + c$ y $b + d$ son pares, pero esto se da cuando a y c tienen la misma paridad

y cuando b y d tienen la misma paridad (es decir ambos son pares o ambos son impares). Definimos entonces los siguientes conjuntos

$$\begin{aligned}
 S_{PP} &= \{(x, y) : x \text{ es par y } y \text{ es par}\} \\
 S_{IP} &= \{(x, y) : x \text{ es impar y } y \text{ es par}\} \\
 S_{PI} &= \{(x, y) : x \text{ es par y } y \text{ es impar}\} \\
 S_{II} &= \{(x, y) : x \text{ es impar y } y \text{ es impar}\}
 \end{aligned}$$

En este caso hay 5 puntos en el grafo y cada uno pertenece a uno de los 4 conjuntos que acabamos de definir. Por el principio del palomar concluimos que hay al menos dos elementos en uno de estos dos conjuntos, y por lo tanto hay por lo menos dos puntos cuyas coordenadas tienen la misma paridad y su punto medio es un elemento de \mathbb{Z}^2 . En la Figura 2.2 presentamos un ejemplo de lo explicado anteriormente. En las dos primeras gráficas tenemos cinco puntos en \mathbb{Z}^2 y el grafo completo generado por los puntos. En la tercera gráfica los puntos verdes representan los puntos medios de cada segmento y el punto rojo representa el punto medio que pertenece a \mathbb{Z}^2 . Este punto verde corresponde al segmento que une los puntos $F = (3, 2)$ y $C = (1, -2)$, que pertenecen a S_{IP} .

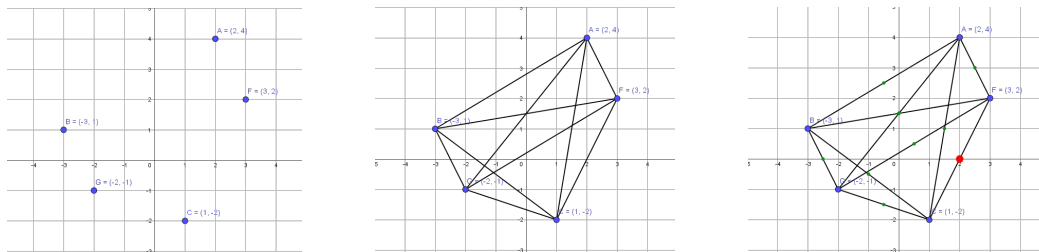


Figura 2.2: Cinco puntos en \mathbb{Z}^2 , el grafo completo generado y puntos medios de los segmentos.

□



Figura 2.3: Palomar

En los ejemplos anteriores usamos dos formas del principio del palomar. En el primer ejemplo definimos formalmente la función f , su dominio y su codominio, mientras que en el segundo ejemplo definimos conjuntos y contrastamos el número de conjuntos con la cantidad de elementos que se deben ubicar en cada uno de ellos. La segunda forma es un poco más intuitiva y es la forma que le da el nombre al principio del palomar. Un palomar es el lugar en que se crían palomas (Figura 2.3) y en este caso el enunciado es

equivalente a la afirmación "Si hay más palomas que palomares, habrá un palomar con más de una paloma". Estas dos formas del principio del palomar se usan ampliamente en matemáticas de acuerdo a la conveniencia para resolver el problema.

Ahora presentamos una generalización del principio del palomar y su demostración.

Teorema 74 (Generalización del principio del palomar). Sea f una función entre dos conjuntos finitos X y Y . Suponga que $|X| = n$ y $|Y| = m$ y que $n > m$. Sea $k = \lceil \frac{n}{m} \rceil$. Entonces existen al menos k elementos $a_1, a_2, \dots, a_k \in X$ tales que

$$f(a_1) = f(a_2) = \dots = f(a_k).$$

Demostración. Esta prueba será por contradicción. Sea $Y = \{y_1, y_2, \dots, y_m\}$ y suponga que para cada $i = 1, \dots, m$ el conjunto $f^{-1}(y_i)$ tiene máximo $k - 1$ elementos, esto implica que

$$|X| = |f^{-1}(y_1)| + |f^{-1}(y_2)| + \dots + |f^{-1}(y_m)| \leq m(k - 1) < m \left(\frac{n}{m} \right) = n$$

Lo que contradice la hipótesis de la cardinalidad de $|X|$. □

2.1.2 Aplicaciones

En esta sección vamos a presentar dos aplicaciones del principio del palomar en la demostración de otros teoremas en matemáticas. Primero presentaremos el teorema de Dirichlet y posteriormente el teorema de emparejamiento de Hall.

Teorema de Dirichlet

Teorema 75 (Teorema de Dirichlet). Para todo número real x y todo entero $Q > 1$, existen enteros p y q con $0 < q < Q$, tales que

$$|qx - p| \leq \frac{1}{Q}$$

Demostración. Consideremos el intervalo $[0, 1)$ con la partición

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \dots, \left[\frac{Q-1}{Q}, 1\right).$$

Esta partición tiene Q elementos y cada intervalo tiene longitud $\frac{1}{Q}$.

Consideremos ahora los siguientes $Q - 1$ números

$$\{x\}, \{2x\}, \{3x\}, \dots, \{(Q - 1)x\}$$

donde $\{a\}$ denota la parte fraccionaria de a , es decir $\{x\} = x - \lfloor x \rfloor$. Cada número $\{kx\}$ pertenece a un intervalo de la partición, sin embargo no podemos aplicar el principio del palomar pues hay más intervalos en la partición que números en nuestra lista. Vamos entonces a considerar tres casos

- Caso 1: $\{kx\} \in \left[\frac{Q-1}{Q}, 1\right)$ para algún k . En este caso

$$|1 - \{kx\}| \leq \frac{1}{Q}$$

Pero $\{kx\} = kx - \lfloor kx \rfloor$, por lo tanto

$$|1 - (kx - \lfloor kx \rfloor)| \leq \frac{1}{Q}$$

Tomando $q = k$ y $p = 1 - \lfloor kx \rfloor$ tenemos el resultado que buscamos.

- Caso 2: $\{kx\} \in \left[0, \frac{1}{Q}\right)$ para algún k . En este caso

$$|\{kx\}| \leq \frac{1}{Q}$$

es decir

$$|kx - \lfloor kx \rfloor| \leq \frac{1}{Q}$$

y tomando $q = k$ y $p = \lfloor kx \rfloor$ se obtiene el resultado.

- Caso 3: Si ninguno de los $Q - 1$ números está en los intervalos de los extremos entonces, deben estar en los $Q - 2$ intervalos restantes. Utilizando el principio del palomar podemos concluir que hay un intervalo de la partición que contiene por lo menos dos elementos de la lista. Supongamos que $\{kx\}$ y $\{jx\}$ están en el mismo intervalo, entonces

$$\frac{1}{Q} > |\{kx\} - \{jx\}| = |(kx - \lfloor kx \rfloor) - (jx - \lfloor jx \rfloor)|$$

y tomando $q = k - j$ y $p = \lfloor kx \rfloor - \lfloor jx \rfloor$ se obtiene el resultado.

□

Observación: En el teorema anterior se puede garantizar que p y q sean primos relativos, ¿cómo se pueden encontrar?

Ahora, utilizando el teorema de Dirichlet podemos probar un criterio para determinar si un número real es irracional.

Teorema 76. Un número real α es irracional si, y solo si, existen sucesiones de enteros p_1, p_2, \dots y q_1, q_2, \dots tal que

$$\lim_{n \rightarrow \infty} q_n \alpha - p_n = 0$$

y $q_n \alpha - p_n \neq 0$ para todo $n \in \mathbb{N}$.

Demostración. [\Rightarrow] Si α es irracional, entonces por el teorema de Dirichlet tenemos que para cada n existen enteros p_n y q_n tales que $|q_n \alpha - p_n| < \frac{1}{n}$. Como $p_n, q_n \in \mathbb{Z}$ se tiene que $q_n \alpha - p_n \neq 0$ y adicionalmente

$$\lim_{n \rightarrow \infty} q_n \alpha - p_n = 0.$$

[\Leftarrow] Supongamos ahora que $q_n \alpha - p_n \neq 0$ y $\lim_{n \rightarrow \infty} q_n \alpha - p_n = 0$ para unas sucesiones $\{p_n\}_{n \in \mathbb{N}}$ y $\{q_n\}_{n \in \mathbb{N}}$. Probaremos que α es irracional por contradicción. Si $\alpha = \frac{a}{b}$ con $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces

$$|q_n \alpha - p_n| = \left| q_n \frac{a}{b} - p_n \right| = \left| \frac{q_n a - p_n b}{b} \right| \geq \frac{1}{b}$$

pues $q_n \alpha - p_n \neq 0$ y $q_n a - p_n b \in \mathbb{N}$, pero esto contradice la hipótesis del límite. Por lo tanto α debe ser irracional. □

Utilizando este criterio podemos dar una nueva prueba de la irracionalidad de $\sqrt{2}$

Corolario 77. $\sqrt{2}$ es irracional.

Demostración. Para probar que es irracional, debemos encontrar dos sucesiones $\{p_n\}_{n \in \mathbb{N}}$ y $\{q_n\}_{n \in \mathbb{N}}$ que satisfagan las condiciones del teorema.

Dado $n \in \mathbb{N}$ consideremos

$$\left(\sqrt{2} - 1\right)^n = \sum_{i=0}^n (-1)^i \binom{n}{i} \left(\sqrt{2}\right)^{n-i}$$

Si el exponente $n-i$ es par, entonces $\left(\sqrt{2}\right)^{n-i}$ es un entero, en el otro caso tenemos que $\left(\sqrt{2}\right)^{n-i}$ se puede escribir como $2^{\frac{n-i-1}{2}} \sqrt{2}$, es decir que la expresión original se puede escribir como

$$\left(\sqrt{2} - 1\right)^n = q_n \sqrt{2} - p_n$$

donde q_n y p_n se obtienen al hacer las simplificaciones correspondientes. Veamos ahora que estas sucesiones satisfacen las condiciones del teorema:

- $\lim_{n \rightarrow \infty} q_n \sqrt{2} - p_n = \lim_{n \rightarrow \infty} (\sqrt{2} - 1)^n = 0$ pues $|\sqrt{2} - 1| < 1$. Por lo tanto se cumple la condición del límite.
- Claramente $q_n \sqrt{2} - p_n \neq 0$ pues $(\sqrt{2} - 1)^n \neq 0$.

Utilizando el teorema anterior podemos concluir que $\sqrt{2}$ es irracional. \square

Teorema de emparejamiento de Hall

El teorema de emparejamiento de Hall o teorema de matrimonio de Hall es un resultado de teoría de grafos que establece una condición para determinar si un grafo tiene un emparejamiento perfecto. Para demostrar este teorema y un corolario usaremos el principio del palomar, pero antes daremos algunas definiciones de teoría de grafos.

Definición 78. Un **grafo** G está determinado por dos conjuntos V y A donde A está formado por parejas de la forma $\{u, v\}$ con $u, v \in V$. El conjunto V se denomina conjunto de vértices o nodos y el conjunto A se denomina conjunto de aristas.

Un grafo $G = (V, A)$ se puede representar gráficamente con un punto por cada elemento de V y una línea por cada elemento de A , es decir, cada par $\{u, v\} \in A$ se representa con una línea cuyos extremos son los puntos u y v .

Definición 79. Dado un grafo $G = (V, A)$, se dice que dos vértices u y v son **adyacentes** si el par $\{u, v\} \in A$. Adicionalmente, dado un vértice $u \in V$, se define la vecindad de u en G como el siguiente conjunto

$$N_G(u) := \{v \in V : v \text{ es adyacente a } u\}$$

La definición de vecindad de un elemento se puede extender para definir la vecindad de un conjunto de la siguiente forma: Dado un subconjunto de vértices $S \subset V$ se define la vecindad de S como

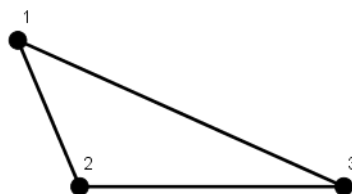
$$N_G(S) := \{v \in V : v \text{ es adyacente a } u \text{ para algún } u \in S\}$$

Ahora presentaremos la definición de un grafo bipartito, que es el objeto fundamental en el teorema de Hall.

Definición 80. Se dice que un grafo $G = (V, A)$ es **bipartito** si su conjunto de vértices V se puede descomponer en dos conjuntos V_1 y V_2 de tal forma que $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \emptyset$ y todas las aristas del grafo tienen un elemento en V_1 y otro elemento en V_2 .

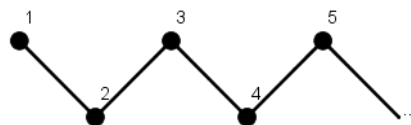
Ejemplos

- (i) Considere el grafo G_1 dado por los siguientes conjuntos $V = \{1, 2, 3\}$, $A = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Este grafo se representa gráficamente como



En este grafo $N_{G_1}(1) = \{2, 3\}$. Este grafo no es bipartito, es decir, el conjunto de vértices no se puede descomponer en dos conjuntos disyuntos que satisfagan la condición de la definición.

- (ii) Definimos G_2 como el grafo determinado por los conjuntos $V = \mathbb{N}$ y $A = \{\{n, n + 1\} : n \in \mathbb{N}\}$. Gráficamente G_2 se representa como



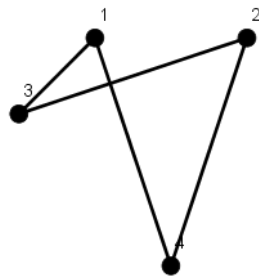
Notemos que si $n > 1$, entonces $N_G(n) = \{n - 1, n + 1\}$. Este grafo es bipartito: tomando $V_1 = \{n \in \mathbb{N} : n \text{ es impar}\}$ y $V_2 = \{n \in \mathbb{N} : n \text{ es par}\}$ se satisface que $V_1 \cap V_2 = \emptyset$, $V_1 \cup V_2 = \mathbb{N}$ y además cada arista en G_2 tiene un extremo en V_1 y otro extremo en V_2 .

- (iii) Considere el grafo G_3 definido por los conjuntos $V = \{1, 2, 3, 4\}$ y $A = \{\{1, 3\}, \{2, 3\}, \{2, 4\}, \{1, 4\}\}$

En este grafo $N_{G_3}(2) = \{3, 4\}$. Este grafo no es bipartito.

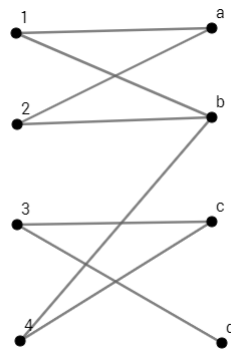
Definimos ahora un emparejamiento perfecto en un grafo bipartito

Definición 81. Dado un grafo bipartito $G = (V, A)$ con partición V_1, V_2 se define un **emparejamiento perfecto** como una función biyectiva $f : V_1 \rightarrow V_2$ tal que para todo $x \in V_1$ se satisface que $\{x, f(x)\} \in A$



Ejemplos

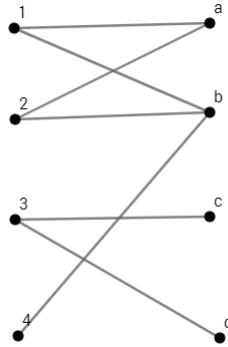
- Considere el siguiente grafo bipartito



En este grafo la función $f : V_1 \rightarrow V_2$ definida por $f(1) = a$, $f(2) = b$, $f(3) = d$ y $f(4) = c$ es un emparejamiento perfecto.

Otro emparejamiento perfecto para este grafo es la función $g : V_1 \rightarrow V_2$ dada por $g(1) = b$, $g(2) = a$, $g(3) = d$ y $g(4) = c$.

- Considere ahora el siguiente grafo



En este grafo bipartito no es posible construir un emparejamiento perfecto.

Como podemos ver en los ejemplos anteriores, no siempre es posible encontrar un emparejamiento perfecto en un grafo bipartito. El teorema de emparejamiento de Hall presenta una condición necesaria y suficiente para que un grafo tenga un emparejamiento perfecto.

Teorema 82 (Emparejamiento de Hall). Suponga que G es un grafo bipartito con partición V_1, V_2 , entonces G tiene un emparejamiento perfecto si y solo si $|V_1| = |V_2|$ y para cualquier $S \subset V$, completamente contenido en V_1 o completamente contenido en V_2 , se satisface que $|N_G(S)| \geq |S|$.

Demostración. \Rightarrow Si G tiene un emparejamiento perfecto, entonces existe una función biyectiva $f : V_1 \rightarrow V_2$ tal que $\{x, f(x)\} \in A$. Como f es biyectiva, es claro que $|V_1| = |V_2|$, debemos probar que para todo $S \subset V_1$ se tiene que $|N_G(S)| \geq |S|$, pero eso es cierto debido a que $f(S) \subset N_G(S)$, entonces

$$|S| = |f(S)| \leq |N_G(S)|$$

\Leftarrow Esta prueba la haremos por inducción sobre $|V_1|$

- Si $|V_1| = 1$ entonces $|V_2| = 1$ y solo hay una arista, entonces el grafo G tiene un emparejamiento perfecto.
- Supongamos que el resultado se satisface para todos los grafos bipartitos en los que $|V_1| \leq k$, es decir, nuestra hipótesis de inducción es:

Si G es un grafo bipartito con partición V_1, V_2 , tales que $|V_1| = |V_2| \leq k$ y tal que para todo $T \subset V_1$ la desigualdad $|N_G(T)| \geq |T|$ se satisface, entonces G tiene un emparejamiento perfecto.

Debemos probar que esta implicación es cierta también para grafos bipartitos en los que $|V_1| = |V_2| = k + 1$. Sea G uno de estos grafos con la propiedad adicional de que para todo $T \subset V_1$ la desigualdad $|N_G(T)| \geq |T|$ se satisface. Se tienen dos casos

* **Caso 1.** $|T| < |N_G(T)|$ para todo $T \subset V_1$. Considere una arista $\{u, v\}$ de G con $u \in V_1$ y $v \in V_2$ y defina H como el grafo bipartito cuya partición es $V_1 - \{u\}$ y $V_2 - \{v\}$. Probaremos a continuación que H tiene un emparejamiento perfecto.

Por la construcción de H , $|V_1 - \{u\}| = |V_2 - \{v\}| = k$, además dado $S \subset V_1 - \{u\}$ se tiene que

$$|N_H(S)| \geq |N_G(S)| - 1 \geq |S|$$

por lo tanto, usando la hipótesis de inducción, podemos concluir que H tiene un emparejamiento perfecto f .

Usando f podemos definir un emparejamiento perfecto f' para G como

$$f'(x) = \begin{cases} f(x) & \text{si } x \neq u \\ v & \text{si } x = u \end{cases}$$

* **Caso 2.** $|T^*| = |N_G(T^*)|$ para algún $T^* \subset V_1$. En este caso consideramos los grafos G_{T^*} y H con particiones $(T^*, N_G(T^*))$ y $(V_1 - T^*, V_2 - N_G(T^*))$ respectivamente. Si probamos que cada uno de estos grafos tiene un emparejamiento perfecto, podemos construir un emparejamiento perfecto para G simplemente uniendo los emparejamientos de G_{T^*} y H . Veamos primero que G_{T^*} tiene un emparejamiento perfecto: Sea $S \subset T^*$, por la definición de G_{T^*} tenemos que $N_G(S) = N_{G_{T^*}}(S)$ y usando la hipótesis de inducción sabemos que $|N_G(S)| \geq |S|$, por lo tanto $|N_{G_{T^*}}(S)| \geq |S|$ y esto implica que G_{T^*} tiene un emparejamiento perfecto.

Veamos ahora que H tiene también un emparejamiento perfecto: Como $|T^*| = |N_G(T^*)|$, es claro que $|V_1 - T^*| = |V_2 - N_G(T^*)|$. Considere ahora $S \subset V_1 - T^*$, $N_H(S) = N_G(T^* \cup S) - N_G(T^*)$, entonces

$$|N_H(S)| \geq |N_G(T^* \cup S)| - |N_G(T^*)| \geq |T^* \cup S| - |T^*| \geq |S|,$$

donde la última desigualdad se satisface porque $T^* \cap S = \emptyset$, y por hipótesis de inducción concluimos que H tiene un emparejamiento perfecto. Ahora, uniendo los emparejamientos de G_S y H obtenemos un emparejamiento perfecto para G que era lo que buscábamos.

□

2.1.3 Ejercicios

- (i) Demuestre que si X es un subconjunto de $\{1, 2, \dots, 2n+1\}$, de cardinal $n+2$, y m es el mayor elemento en X , entonces existen $i, j \in X$ tales que $m = i+j$ y $i \neq j$.

Sugerencia. Para cada elemento $k \in X - \{m\}$ defina la función

$$a_k = \begin{cases} k & \text{si } k \leq \frac{m}{2} \\ m - k & \text{si } k > \frac{m}{2} \end{cases}$$

y estudie su dominio y rango.

- (ii) Un rectángulo de 3×7 se divide en 21 cuadrados de lado 1 que son coloreados de rojo o negro. Pruebe que el rectángulo original contiene un rectángulo no trivial (es decir, diferente de $k \times 1$ o $1 \times k$) cuyas esquinas tienen el mismo color.
- (iii) Sea G un grafo con $2n$ vértices tal que cada vértice tiene grado por lo menos n . Probar que G tiene un emparejamiento perfecto. Recuerde que en un grafo (no dirigido), el grado de un vértice v corresponde al cardinal de $N_G(v)$.

2.2 Fractales

La geometría fractal es un área de las matemáticas que ha tenido un amplio desarrollo en los últimos 40 años debido a que estudia objetos que no se modelan de forma apropiada con la geometría clásica. Estos objetos aparecen constantemente en la naturaleza y se caracterizan por tener un patrón que se repite al observar el objeto a diferentes escalas, por ejemplo, en un relámpago podemos ver que una rama del relámpago es similar al relámpago completo.



En matemáticas, es posible construir conjuntos fractales haciendo modificaciones sucesivas a un conjunto. A continuación veremos tres ejemplos.

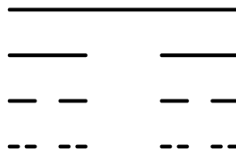
Conjunto de Cantor

El conjunto de Cantor está contenido en \mathbb{R} y se construye de la siguiente forma:

- Definimos el conjunto E_0 como el intervalo $[0, 1]$
- E_1 es el conjunto obtenido al borrar el tercio de E_0 que está en el medio, es decir, $E_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$
- En general el conjunto E_K se obtiene al remover de cada intervalo en E_{k-1} el intervalo de la mitad.
- El conjunto de Cantor F se define como la intersección de todos los conjuntos E_k , es decir,

$$F := \bigcap_{k=0}^{\infty} E_k$$

Gráficamente cada iteración del conjunto de Cantor se representa como

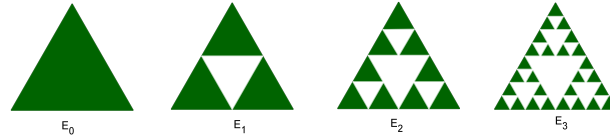


Triángulo de Sierpinski

El triángulo de Sierpinski está contenido en \mathbb{R}^2 . La construcción se hace de la siguiente forma

- El conjunto E_0 corresponde a un triángulo equilátero de lado 1.
- El conjunto E_1 se construye eliminando del conjunto E_0 el triángulo obtenido al unir los puntos medios de cada lado. Esto genera 3 triángulos equiláteros con lados de longitud $\frac{1}{2}$.
- El conjunto E_k se obtiene al eliminar de cada triángulo del conjunto E_{k-1} el triángulo obtenido al unir los puntos medios de cada lado.
- El triángulo de Sierpinski es la intersección de todos los E_k , es decir, $F := \bigcap_{k=0}^{\infty} E_k$

A continuación tenemos la representación gráfica del triángulo de Sierpinski.

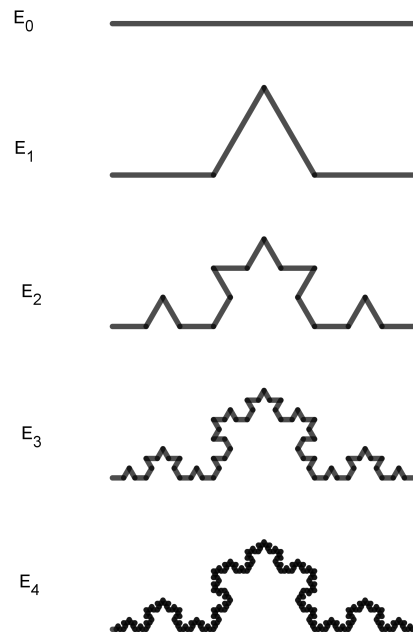


Curva de Koch

La curva de Koch está contenida en \mathbb{R}^2 y se contruye de la siguiente forma:

- Se define el conjunto E_0 como el intervalo cerrado $[0, 1]$
- El conjunto E_1 se obtiene reemplazando el tercio medio del intervalo por los lados de un triángulo equilátero cuya base es el intervalo que se eliminó.
- El conjunto E_k se obtiene al reemplazar el tercio medio de cada segmento de E_{k-1} por los lados del triángulo equilátero cuya base es el segmento eliminado.
- La curva de Koch F corresponde al conjunto $F := \lim_{k \rightarrow \infty} E_k$

Gráficamente cada iteración se representa de la siguiente forma



Los ejemplos anteriores tienen varias características en común. Por ejemplo, se pueden definir de forma recursiva y cada iteración corresponde a un procedimiento sencillo de ejecutar, además el conjunto en su totalidad es similar a sus partes. Esta última característica se denomina autosimilitud y es una característica especial de los conjuntos fractales. Si en el conjunto de Cantor nos restringimos solo a los conjuntos obtenidos a partir del intervalo $[0, \frac{1}{3}]$ en la primera iteración, obtenemos un conjunto que geoméricamente es igual al conjunto original.

Otra característica de los ejemplos presentados anteriormente es que la dimensión de ellos no es entera; si analizamos la curva de Koch notamos que, aunque está contenida en \mathbb{R}^2 , no es un conjunto de dimensión 2 y, además, su longitud es infinita, entonces intuitivamente es un conjunto cuya dimensión está entre 1 y 2. Las características mencionadas anteriormente son justamente las que permiten distinguir los fractales de otros objetos de la geometría clásica. En las siguientes secciones presentaremos dos formas de definir la dimensión de un fractal y calcularemos las dimensiones de los ejemplos anteriores.

2.2.1 Preliminares

Empezaremos recordando algunos conceptos de teoría de la medida que nos permitirán estudiar la dimensión de un fractal y la propiedad de autosimilitud.

Definición 83. Decimos que una función μ es una medida en \mathbb{R}^n si satisface las siguientes condiciones

- (i) $\mu(A) \geq 0$ para todo $A \subset \mathbb{R}^n$
- (ii) $\mu(\emptyset) = 0$
- (iii) $\mu(A) \leq \mu(B)$ si $A \subset B$
- (iv) Dada una sucesión finita o enumerable de conjuntos A_1, A_2, \dots entonces

$$\mu \left(\bigcup_{i=1}^{\infty} A_i \right) \leq \sum_{i=1}^{\infty} \mu(A_i)$$

donde la igualdad se da si los conjuntos son Borel y son disjuntos dos a dos.

Intuitivamente la medida de un conjunto indica su tamaño. Las condiciones de la definición indican que el tamaño de un conjunto se puede obtener sumando los tamaños de sus partes y, además, que la medida es una función creciente con respecto a la inclusión de conjuntos. Cuando la medida es una función acotada, nos referimos a ella como una distribución de masa.

Definición 84. Una medida μ en un conjunto acotado de \mathbb{R}^n tal que $0 < \mu(\mathbb{R}^n) < \infty$ se denomina una distribución de masa y el valor $\mu(A)$ se denomina la masa de A .

Ejemplos

- (i) **Medida de conteo:** Para cada subconjunto A de \mathbb{R}^n se define $\mu(A) = |A|$ si A es finito y se define $\mu(A) = \infty$ en otro caso.
- (ii) **Medida concentrada en un punto:** Dado un punto a en \mathbb{R}^n se define μ de la siguiente forma:

$$\mu(A) = \begin{cases} 1 & \text{si } a \in A \\ 0 & \text{si } a \notin A \end{cases}$$

Esta medida es una distribución de masa.

(iii) **Medida de Lebesgue en \mathbb{R} :** Dado un subconjunto A de \mathbb{R} , la medida de Lebesgue de A , denotada $\mathcal{L}(A)$, se define de la siguiente forma:

- Si $A = [a, b]$ entonces $\mathcal{L}(A) = b - a$
- Si $A = \bigcup_{i=0}^{\infty} [a_i, b_i]$ es una unión finita o enumerable de intervalos disjuntos, entonces la medida de Lebesgue de A se define como

$$\mathcal{L}(A) = \sum_{i=0}^{\infty} (b_i - a_i)$$

- Si A es un conjunto arbitrario de \mathbb{R} entonces

$$\mathcal{L}(A) = \inf \left\{ \sum_{i=0}^{\infty} (b_i - a_i) : A \subset \bigcup_{i=0}^{\infty} [a_i, b_i] \right\}$$

Intuitivamente la medida de Lebesgue de un conjunto indica su longitud. Si el conjunto es un intervalo esto es evidente pero para un conjunto arbitrario la medida encuentra el ínfimo de las longitudes de los conjuntos formados por intervalos que lo contienen. Notemos que la medida de Lebesgue de un conjunto finito es cero.

2.2.2 Dimensión fractal

Como mencionamos anteriormente, los conjuntos fractales no tienen dimensión entera y ésta es una de sus características fundamentales. Sin embargo, hay varias formas de definir la dimensión de un conjunto. En esta sección presentaremos la dimensión por cajas y la dimensión de Hausdorff de un conjunto.

Dimensión de Hausdorff

Para definir la dimensión de Hausdorff de un conjunto primero presentamos la medida de Hausdorff, posteriormente definimos la dimensión y finalmente presentamos algunos ejemplos.

Medida de Hausdorff

La medida de Hausdorff se define a partir de δ -cubrimientos. Empezaremos con esta definición y luego procedemos a definir la medida de Hausdorff.

Definición 85. Sea U un subconjunto de \mathbb{R}^n . Se define el diámetro de U , denotado $|U|$, como

$$|U| = \sup\{|x - y| : x, y \in U\}$$

Definición 86. Si $\{U_i\}_{i=1}^{\infty}$ es una colección de conjuntos tales que $|U_i| < \delta$ y $F \subset \bigcup_{i=1}^{\infty} U_i$, decimos que $\{U_i\}_{i=1}^{\infty}$ es un δ -cubrimiento de F .

Ahora pasamos a la definición de medida de Hausdorff de un subconjunto de \mathbb{R}^n

Definición 87. Sean $F \subset \mathbb{R}^n$ y $s \geq 0$. Para cada $\delta > 0$ se define $\mathcal{H}_{\delta}^s(F)$ como

$$\mathcal{H}_{\delta}^s(F) = \inf \left\{ \sum_{i=1}^{\infty} |U_i|^s : \{U_i\}_{i=1}^{\infty} \text{ es un } \delta\text{-cubrimiento de } F \right\}$$

Se define la medida s -dimensional de Hausdorff del conjunto F como

$$\mathcal{H}^s(F) = \lim_{\delta \rightarrow 0} \mathcal{H}_{\delta}^s(F)$$

En la definición anterior el valor de $\mathcal{H}_{\delta}^s(F)$ crece cuando δ disminuye, por lo tanto el límite siempre existe (puede ser ∞). Notemos que si F es un conjunto Borel de \mathbb{R}^n , entonces $\mathcal{H}^0(F)$ corresponde al número de puntos de F y, si F es una curva suave, $\mathcal{H}^1(F)$ corresponde a su longitud.

Probaremos ahora dos propiedades de la medida de Hausdorff que más adelante nos permitirán calcular la dimensión del conjunto de Cantor y del polvo de Cantor.

Proposición 88 (Propiedad de escala). Si $F \subset \mathbb{R}^n$ y $\lambda > 0$ entonces $\mathcal{H}^s(\lambda F) = \lambda^s \mathcal{H}^s(F)$, donde $\lambda F = \{\lambda x : x \in F\}$, es decir, λF es el conjunto F a escala λ .

Demostración. En esta prueba primero demostraremos que $\mathcal{H}_{\lambda\delta}^s(\lambda F) = \lambda^s \mathcal{H}_{\delta}^s(F)$ y luego, tomando el límite cuando $\delta \rightarrow 0$, obtenemos el resultado. Sea $\{U_i\}_{i=1}^{\infty}$ un δ -cubrimiento de F . Por la definición de δ -cubrimiento y de λF se tiene que $\{\lambda U_i\}_{i=1}^{\infty}$ es un $\lambda\delta$ -cubrimiento de λF y con este $\lambda\delta$ cubrimiento de λF tenemos

$$\mathcal{H}_{\lambda\delta}^s(\lambda F) \leq \sum_{i=1}^{\infty} |\lambda U_i|^s = \lambda^s \sum_{i=1}^{\infty} |U_i|^s$$

Esto se satisface para cualquier δ -cubrimiento de F , entonces por la definición de $\mathcal{H}_{\delta}^s(F)$ como un ínfimo, concluimos que $\mathcal{H}_{\lambda\delta}^s(\lambda F) \leq \lambda^s \mathcal{H}_{\delta}^s(F)$.

Por otro lado

$$\mathcal{H}_{\delta}^s(F) \leq \sum_{i=1}^{\infty} |U_i|^s = \frac{1}{\lambda^s} \sum_{i=1}^{\infty} |\lambda U_i|^s.$$

Entonces, como la colección de conjuntos $\{\lambda U_i\}_{i=1}^{\infty}$ es un $\lambda\delta$ -cubrimiento de λF y $\mathcal{H}_{\delta}^s(F)$ es un ínfimo, se satisface que $\mathcal{H}_{\delta}^s(F) \leq \frac{1}{\lambda^s} \mathcal{H}_{\lambda\delta}^s(\lambda F)$.

Concluimos así que $\mathcal{H}_{\delta}^s(F) = \frac{1}{\lambda^s} \mathcal{H}_{\lambda\delta}^s(\lambda F)$ y tomando el límite cuando $\delta \rightarrow 0$ obtenemos $\mathcal{H}^s(\lambda F) = \lambda^s \mathcal{H}^s(F)$ que era lo que queríamos probar. □

Proposición 89. Sean $F \subset \mathbb{R}^n$ y $f : F \rightarrow \mathbb{R}^m$ una función tal que

$$|f(x) - f(y)| \leq c|x - y|^\alpha$$

para todo $x, y \in F$ y para constantes $c > 0$ y $\alpha > 0$. Entonces para cada s se satisface que

$$\mathcal{H}_\alpha^{\frac{s}{\alpha}}(f(F)) \leq c^{\frac{s}{\alpha}} \mathcal{H}^s(F)$$

Demostración. Sea $\{U_i\}_{i=1}^\infty$ un δ -cubrimiento de F . La colección $\{f(U_i \cap F)\}_{i=1}^\infty$ es un cubrimiento de $f(F)$, pero adicionalmente es un $c\delta^\alpha$ -cubrimiento. Dado que f satisface la desigualdad de la hipótesis se tiene que

$$\begin{aligned} |f(x) - f(y)| &\leq \sup\{c|x - y|^\alpha : x, y \in U_i\} \\ \sup\{|f(x) - f(y)| : x, y \in U_i\} &\leq \sup\{c|x - y|^\alpha : x, y \in U_i\} \\ |f(U_i)| &\leq c \cdot \sup\{|x - y|^\alpha : x, y \in U_i\} \\ |f(U_i)| &\leq c \cdot \sup\{|x - y| : x, y \in U_i\}^\alpha \\ |f(U_i)| &\leq c|U_i|^\alpha \\ |f(U_i)| &\leq c\delta^\alpha. \end{aligned}$$

Esto implica que $\{f(U_i \cap F)\}_{i=1}^\infty$ es un $c\delta^\alpha$ -cubrimiento de $f(F)$ y por lo tanto

$$\mathcal{H}_{c\delta^\alpha}^{\frac{s}{\alpha}}(f(F)) \leq \sum_i |f(U_i \cap F)|^{\frac{s}{\alpha}} \leq \sum_i c^{\frac{s}{\alpha}} |U_i|^s = c^{\frac{s}{\alpha}} \sum_i |U_i|^s$$

para todo δ -cubrimiento de F . Esto implica $\mathcal{H}_{c\delta^\alpha}^{\frac{s}{\alpha}}(f(F)) \leq c^{\frac{s}{\alpha}} \mathcal{H}_\delta^s(F)$ y tomando el límite cuando δ tiende a 0 obtenemos

$$\mathcal{H}_\alpha^{\frac{s}{\alpha}}(f(F)) \leq c^{\frac{s}{\alpha}} \mathcal{H}^s(F)$$

que era lo que se quería probar. \square

Dimensión de Hausdorff

Dado un conjunto F y un $\delta < 1$ fijo, la medida de Hausdorff s dimensional es no-creciente con respecto a s , esto implica que cuando $t > s$ y $\{U_i\}_{i=1}^\infty$ es un δ -cubrimiento entonces $\sum_{i=1}^\infty |U_i|^t \leq \delta^{t-s} \mathcal{H}_\delta^s(F)$ y por lo tanto $\mathcal{H}_\delta^t(F) \leq \delta^{t-s} \mathcal{H}_\delta^s(F)$.

Definición 90 (Dimensión de Hausdorff). Dado un conjunto F , se define la dimensión de Hausdorff de F como

$$\dim_H(F) := \inf\{s : \mathcal{H}^s(F) = 0\}$$

La dimensión de Hausdorff también se puede definir como el supremo de las dimensiones en las que el conjunto F tiene medida de Hausdorff infinita, es decir,

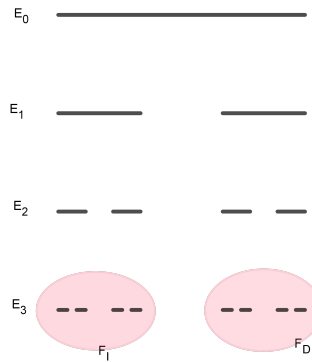
$$\dim_H(F) = \sup\{s : \mathcal{H}^s(F) = \infty\}$$

de forma tal que $\mathcal{H}^s(F) = \infty$ si $s < \dim_H(F)$ y $\mathcal{H}^s(F) = 0$ si $s > \dim_H(F)$.

Ejemplos

- El conjunto de Cantor tiene dimensión de Hausdorff igual a $\frac{\log 2}{\log 3}$.

Demostración. Para probar que la dimensión de Hausdorff del conjunto de Cantor es $\frac{\log 2}{\log 3}$ primero observamos que el conjunto de Cantor está formado por dos copias similares al conjunto completo, es decir, geoméricamente los puntos del conjunto de Cantor que son menores que $\frac{1}{2}$ forman un conjunto igual al conjunto total pero a una escala de $\frac{1}{3}$; lo mismo ocurre con los puntos del conjunto de Cantor que son mayores a $\frac{1}{2}$. Esto implica que podemos escribir el conjunto de Cantor F como la unión disjunta de dos conjuntos iguales F_I y F_D que son una copia a escala de F .



Ahora, utilizando la propiedad de escala de la dimensión de Hausdorff obtenemos la siguiente identidad

$$\mathcal{H}^s(F) = \mathcal{H}^s(F_I) + \mathcal{H}^s(F_D) = \frac{1}{3^s} \mathcal{H}^s(F) + \frac{1}{3^s} \mathcal{H}^s(F)$$

Esto implica que

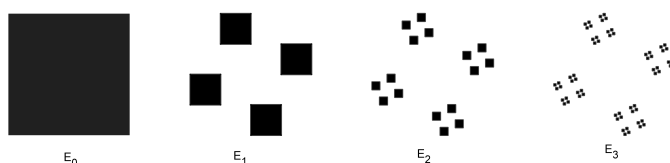
$$1 = \frac{1}{3^s} + \frac{1}{3^s}$$

y por lo tanto $s = \frac{\log 2}{\log 3}$.

La demostración anterior es intuitiva y no utiliza la definición de medida en términos de δ -cubrimientos, en su lugar utiliza la propiedad de escala para demostrar el resultado, sin embargo se puede usar la definición de medida de Hausdorff para probar que $\frac{1}{2} \leq \mathcal{H}^s(F) \leq 1$. Esto se deja como ejercicio para el lector.

□

- El polvo de Cantor es un fractal que se define con un procedimiento análogo al del conjunto de Cantor. El conjunto inicial E_0 es un cuadrado de lado 1. Este cuadrado se divide en 16 partes iguales y se conservan 4 de los cuadrados obtenidos de la forma en que se muestra en la imagen, obteniendo el conjunto E_1 . En general el conjunto E_k se obtiene al dividir los cuadrados del conjunto E_{k-1} y conservando 4 de ellos en la forma indicada en las imágenes. El polvo de Cantor F corresponde a $\bigcap_{k=0}^{\infty} E_k$



Este fractal tiene dimensión de Hausdorff mayor o igual a 1 y menor o igual a $\sqrt{2}$.

Demostración. Denotemos el polvo de Cantor por F . Si tomamos $\delta = \frac{\sqrt{2}}{4^k}$, tenemos que los cuadrados del conjunto E_k son un δ -cubrimiento de F , por lo tanto $\mathcal{H}_\delta^1(F) \leq \sum_{i=1}^{4^k} \frac{\sqrt{2}}{4^k} = \sqrt{2}$. Ahora, dado que cuando δ tiende a 0, k tiende a infinito, concluimos que $\mathcal{H}^1(F) \leq \sqrt{2}$.

Probaremos ahora que $1 \leq \mathcal{H}^1(F)$. Para probar esta desigualdad vamos a estudiar la proyección π_1 sobre la primera componente. Esta proyección es una función Lipschitz, es decir,

$$|\pi_1(x_1, y_1) - \pi_1(x_2, y_2)| \leq |(x_1, y_1) - (x_2, y_2)|$$

Utilizando esta condición, la segunda propiedad de la medida de Hausdorff y el hecho de que $\pi_1(F) = [0, 1]$, concluimos lo siguiente

$$1 = \text{longitud de } [0, 1] = \mathcal{H}^1([0, 1]) = \mathcal{H}^1(\pi_1(F)) \leq \mathcal{H}^1(F)$$

Con esta desigualdad mostramos el resultado. □

2.2.3 Dimensión por cajas (Box counting)

El método de conteo de cajas para encontrar la dimensión de un subconjunto F de \mathbb{R}^n es el siguiente:

- Considere una malla formada por cajas de lado δ
- Defina $M_\delta(F)$ como el número de cajas en la malla que intersectan a F , es decir, $M_\delta(F)$ es el número de cajas necesario para cubrir F .

Ahora, se definen la dimensión superior y la dimensión inferior de F como

$$\overline{\dim}_B(F) = \limsup_{\delta \rightarrow 0} \frac{\log M_\delta(F)}{-\log \delta} \quad \text{y} \quad \underline{\dim}_B(F) = \liminf_{\delta \rightarrow 0} \frac{\log M_\delta(F)}{-\log \delta}$$

respectivamente. Si los dos límites coinciden, este valor corresponde a la dimensión por cajas del conjunto F .

Intuitivamente esta dimensión indica qué tanto cambia la figura al observarla a una escala δ . Veamos dos ejemplos

- Si consideramos F como un segmento de recta de longitud 1 podemos comprobar que su dimensión por cajas es 1.

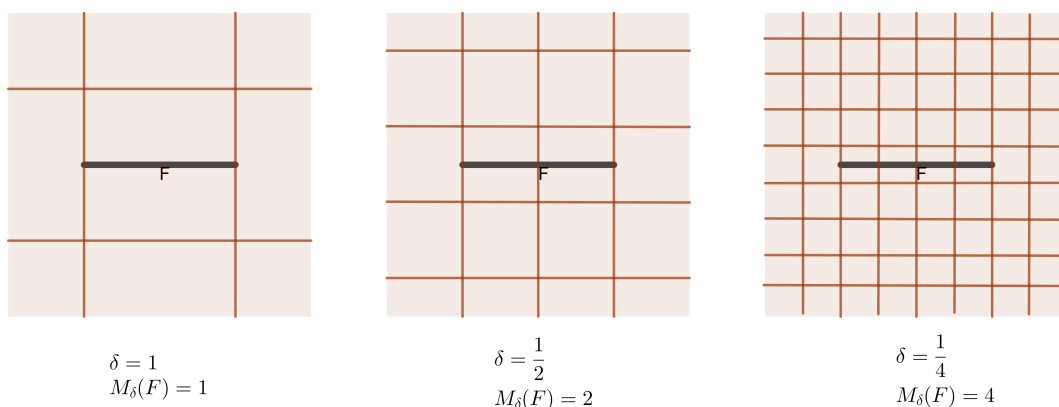


Figura 2.4: Conteo por cajas de un segmento de recta de longitud 1.

En la Figura 2.4 vemos tres mallas de longitudes 1 , $\frac{1}{2}$ y $\frac{1}{4}$ respectivamente, donde podemos contar la cantidad de celdas de la malla que intersectan al segmento. En general, si una malla tiene longitud $\delta = \frac{1}{2^n}$, entonces $M_\delta(F) = 2^n$ y por lo tanto

$$\overline{\dim}_B(F) = \limsup_{\delta \rightarrow 0} \frac{\log 2^n}{-\log \frac{1}{2^n}} = 1$$

y

$$\underline{\dim}_B(F) = \liminf_{\delta \rightarrow 0} \frac{\log 2^n}{-\log \frac{1}{2^n}} = 1.$$

Como el límite superior es igual al límite inferior, concluimos que la dimensión por conteo de cajas de este segmento de recta es igual a 1. Notemos que en este caso basta con considerar una sucesión específica de mallas de diámetros $\frac{1}{2^n}$. Esto se debe a que si una malla tiene diámetro $\delta < 1$, entonces existen k y $k + 1$ tales que $\frac{1}{2^{k+1}} < \delta < \frac{1}{2^k}$ y por lo tanto $M_{\frac{1}{2^{k+1}}}(F)$ y $M_{\frac{1}{2^k}}(F)$ son cotas superior e inferior de $M_\delta(F)$ respectivamente, por lo tanto los límites deben ser iguales.

- La dimensión por cajas del conjunto de cantor es $\frac{\log 2}{\log 3}$.
Para calcular esta dimensión vamos a utilizar mallas de tamaño $\frac{1}{3^n}$. En la figura 2.5 tenemos tres mallas que cubren el conjunto de Cantor F . En la figura podemos ver que $M_1(F) = 1$, $M_{\frac{1}{3}}(F) = 2$ y $M_{\frac{1}{9}}(F) = 4$. En general se tiene que $M_{\frac{1}{3^k}}(F) = 2^k$ y por lo tanto

$$\overline{\dim}_B(F) = \limsup_{n \rightarrow \infty} \frac{\log 2^n}{-\log \frac{1}{3^n}} = \frac{\log 2}{\log 3}$$

y

$$\underline{\dim}_B(F) = \liminf_{n \rightarrow \infty} \frac{\log 2^n}{-\log \frac{1}{3^n}} = \frac{\log 2}{\log 3}.$$

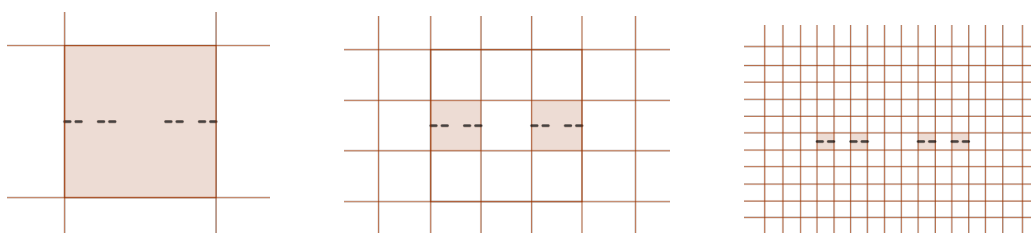


Figura 2.5: Dimensión por conteo de cajas del conjunto de Cantor. Mallas de tamaño 1 , $\frac{1}{3}$ y $\frac{1}{9}$.

De forma análoga al ejemplo anterior, es suficiente considerar solo mallas con tamaños $\frac{1}{3^k}$ dado que para todo δ , existe k tal que $M_\delta(F)$ se puede acotar con $M_{\frac{1}{3^k}}(F)$ y $M_{\frac{1}{3^{k+1}}}(F)$.

Aunque la definición original de esta dimensión está dada por el conteo de intersecciones del conjunto con una malla, existen otras formas equivalentes de calcular la dimensión por cajas de un conjunto. Estas equivalencias se enuncian en la siguiente proposición:

Proposición 91. La dimensión superior e inferior de F se definen como

$$\overline{\dim}_B(F) = \limsup_{\delta \rightarrow 0} \frac{\log M_\delta(F)}{-\log \delta}$$

y

$$\underline{\dim}_B(F) = \liminf_{\delta \rightarrow 0} \frac{\log M_\delta(F)}{-\log \delta}$$

respectivamente, donde $M_\delta(F)$ es cualquiera de las siguientes cantidades

- El menor número de bolas cerradas de radio δ que cubren F .
- El menor número de cubos de lado δ que cubren F .
- El menor número de celdas, de una malla de lado δ , que intersectan a F .
- El menor número de conjuntos de diámetro menor o igual a δ que cubren F .
- El mayor número de bolas disjuntas de radio δ con centros en F .

2.2.4 Ejercicios

- (i) Demostrar que la medida de conteo y la medida concentrada en un punto, definidas previamente en esta sección, son funciones de medida.
- (ii) Calcular la dimensión por cajas de la curva de Koch.
- (iii) Calcular la dimensión por cajas del polvo de Cantor.

2.3 Topología del espacio de matrices

En este capítulo probaremos tres proposiciones relacionadas con la topología que se define sobre el espacio de matrices cuadradas con entradas en \mathbb{R} o en \mathbb{C} . Para esto primero recordaremos los conceptos básicos de topología y posteriormente presentaremos los resultados relacionados con el espacio de matrices.

2.3.1 Conceptos básicos de topología

Definición 92 (Espacio topológico). Dado un conjunto X . Una topología sobre X se define como una colección \mathcal{T} de subconjuntos de X que satisface las siguientes propiedades

- (i) $\emptyset \in \mathcal{T}$ y $X \in \mathcal{T}$.
- (ii) Si U_1, \dots, U_n es una colección finita de elementos de \mathcal{T} , entonces $\bigcap_{i=1}^n U_i \in \mathcal{T}$.
- (iii) Si U_1, U_2, \dots es una colección de elementos de \mathcal{T} , entonces $\bigcup_{i=1}^{\infty} U_i \in \mathcal{T}$.

Esta primera definición corresponde a la construcción básica de esta área de las matemáticas. Cada elemento de \mathcal{T} se denomina **conjunto abierto**. Notemos que en esta definición los conjuntos X y \mathcal{T} pueden ser finitos o infinitos. Además, los items (ii) y (iii) indican que \mathcal{T} es cerrada para uniones arbitrarias e intersecciones finitas. Veamos algunos ejemplos de espacios topológicos.

- (i) Para cualquier conjunto X podemos definir la topología trivial como $\mathcal{T} = \{\emptyset, X\}$. Esta topología es la topología sobre X con menor número de abiertos.
- (ii) Para cualquier conjunto X podemos definir la topología discreta como $\mathcal{T} = \mathcal{P}(X)$, donde $\mathcal{P}(X)$ denota las partes de X . Esta es la topología sobre X con mayor número de abiertos, pues cualquier subconjunto de X es abierto.
- (iii) Dado un conjunto X y un punto $p \in X$, se define la topología punto incluido como $\mathcal{T}_p = \emptyset \cup \{U \subset X : p \in U\}$. Los abiertos en esta topología son los conjuntos que contienen a p .
- (iv) Sobre los números reales se define la topología usual \mathcal{T} como la topología en la que los conjuntos abiertos corresponden a uniones de intervalos de la forma $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.

En general hay una relación importante entre las funciones de medida sobre un conjunto X y un espacio topológico que se puede definir a partir de ellas. Esta relación surge a partir de la siguiente definición

Definición 93. Dados un conjunto X dotado de una función de medida d y $\epsilon > 0$, el conjunto

$$B_\epsilon(x) = \{y \in \mathbb{R}^n : d(x, y) < \epsilon\}$$

se define como la bola abierta con centro x y radio ϵ .

El conjunto de todas las bolas abiertas genera una topología sobre X . En esta topología los abiertos son uniones arbitrarias de bolas abiertas e intersecciones finitas de bolas abiertas. Se dice que esta topología es inducida por la medida d .

2.3.2 Espacio topológico de matrices

Consideremos los conjuntos de matrices cuadradas con entradas reales o con entradas complejas, denotados $M_n(\mathbb{R})$ y $M_n(\mathbb{C})$ respectivamente. Estos conjuntos son anillos cuando se consideran la suma y el producto usual de matrices. Además de la estructura de anillo, estos conjuntos se pueden dotar de una norma que induce la definición de un espacio topológico. A continuación presentaremos la definición de una norma sobre estos espacios de matrices y posteriormente definiremos la métrica y la topología inducidas.

Definición 94. Sea $K = \mathbb{R}$ o $K = \mathbb{C}$. Sobre $M_n(K)$ definimos la norma $\|\cdot\|$ de la siguiente forma

$$\|A\| = \sup \left\{ \frac{|Ax|}{|x|} : x \in K^n \text{ y } x \neq 0 \right\}$$

donde $|\cdot|$ denota la norma usual en K^n

Una definición equivalente de la norma de una matriz se obtiene al calcular el cociente de la definición solo sobre los vectores unitarios, es decir,

$$\|A\| = \sup \{ |Ax| : x \in K^n \text{ y } |x| = 1 \}.$$

A partir de esta norma se puede definir una métrica en $M_n(K)$ de la forma usual y con ella, los abiertos de una topología sobre $M_n(K)$.

Definición 95. • Dadas dos matrices $A, B \in M_n(K)$, definimos la distancia entre ellas como

$$\rho(A, B) = \|B - A\|.$$

- Dada $A \in M_n(K)$ definimos una bola abierta con centro en A y radio ϵ como

$$\mathcal{B}_\epsilon(A) = \{X \in M_n(K) : \|X - A\| < \epsilon\}$$

- Se dice que un conjunto $Y \subset M_n(K)$ es abierto si para toda matriz $A \in Y$ existe $\epsilon > 0$ tal que $\mathcal{B}_\epsilon(A) \subset Y$.

Utilizando estas definiciones podemos probar propiedades importantes de algunos conjuntos especiales de matrices. Estos resultados serán presentados en las proposiciones siguientes.

Proposición 96. El conjunto de matrices invertibles $GL_n(\mathbb{R})$ es un conjunto abierto y denso en $M_n(\mathbb{R})$.

Demostración. Para probar que $GL_n(\mathbb{R})$ es abierto consideramos $\det : M \mapsto \det(M)$ como la función que a cada matriz le asigna su determinante. Dado que esta función es un polinomio en los coeficientes de la matriz, es continua. Note que $GL_n(\mathbb{R}) = \det^{-1}(\mathbb{R}^*)$, pero \mathbb{R}^* es un conjunto abierto en la topología usual de \mathbb{R} , por lo tanto su imagen inversa $GL_n(\mathbb{R})$ es un conjunto abierto también.

Recordemos que en un espacio topológico (X, \mathcal{T}) , un conjunto $N \subset X$ es denso si para todo elemento $x \in X$, la intersección de cualquier abierto V_x que lo contenga y N es no vacía. Notemos que esta definición es equivalente la afirmación de que todo elemento de X se puede aproximar por elementos de N y esto es precisamente lo que vamos a probar en nuestro caso. Considere $A \in M_n(\mathbb{R})$ y $\chi_A(x)$ su polinomio

característico. Por el teorema fundamental del álgebra sabemos que χ_A tiene un número finito de raíces complejas, en particular esto implica que existe $x_0 \in \mathbb{R}^+$ tal que para todo x en el intervalo $(0, x_0)$, $\chi_A(x) \neq 0$. De esto deducimos que existe $p_0 \in \mathbb{N}$ tal que para todo $p \in \mathbb{N}$ con $p \geq p_0$ se tiene que $\det(A - \frac{1}{p}I_n) \neq 0$. Ahora, para cada $p \geq p_0$ sea $A_p = A - \frac{1}{p}I_n$. Cada A_p es invertible, es decir que cada $A_p \in GL_n(\mathbb{R})$. Además, se tiene que $\lim_{p \rightarrow \infty} A_p = A$, esto implica que cada matriz A es el límite de una sucesión de matrices en $GL_n(\mathbb{R})$, por lo tanto $GL_n(\mathbb{R})$ es denso en $M_n(\mathbb{R})$. □

Proposición 97. El espacio de las matrices ortogonales $\mathcal{O}_n(\mathbb{R})$ es compacto.

Demostración. Sea f la función que a cada matriz M la envía en MM^T . Esta función es continua pues es composición de funciones continuas. Además, notemos que $\mathcal{O}_n(\mathbb{R}) = f^{-1}(\{I_n\})$, esto implica que $\mathcal{O}_n(\mathbb{R})$ es un conjunto cerrado pues es la imagen inversa de un conjunto cerrado. Ahora, para probar la compacidad de $\mathcal{O}_n(\mathbb{R})$, basta mostrar que es acotado. Esto lo probaremos teniendo en cuenta que si una matriz es ortogonal entonces sus columnas forman una base ortonormal de \mathbb{R}^n . Para toda matriz $A \in \mathcal{O}_n(\mathbb{R})$ se tiene que $\|A\| \leq C$, donde C es una constante independiente de A , eso implica que $\mathcal{O}(\mathbb{R})$ es acotado. □

Proposición 98. Sea $p \in \{0, 1, \dots, n\}$. El conjunto de matrices de rango menor o igual a p es un conjunto cerrado de $M_n(\mathbb{R})$.

Demostración. Si $p = 0$ o $p = n$ el resultado es evidente. Supongamos entonces que $p \in \{1, \dots, p-1\}$ y sea A una matriz de rango menor o igual a p . Debido al valor del rango de A , tenemos que todos los menores de tamaño mayor o igual a $p+1$ son nulos, entonces si $I, J \subset \{1, \dots, n\}$ con $|I| = |J| = p+1$, y $A_{I,J}$ es la submatriz de A formada por las filas con índices en I y las columnas con índices en J , la aplicación que a cada matriz M le asigna el valor $\det(M_{I,J})$ es continua, pues es composición de funciones continuas. Notemos ahora que $f_{I,J}^{-1}(\{0\}) = \{A \in M_n(\mathbb{R}) : \det(A_{I,J}) = 0\}$ es la imagen inversa de un conjunto cerrado, por lo tanto es un conjunto cerrado también. Esto implica que el conjunto de matrices de rango menor o igual a p es un conjunto cerrado pues es la intersección finita de conjuntos cerrados. □

Proposición 99. El conjunto de matrices diagonalizables en $M_n(\mathbb{C})$ es denso en $M_n(\mathbb{C})$. Este resultado no es cierto en $M_n(\mathbb{R})$.

Demostración. Sea $A \in M_n(\mathbb{C})$ y sea $sp(A)$ el conjunto de valores propios $\{\lambda_i\}_{1 \leq i \leq n}$. El teorema de Schur garantiza que A es similar a una matriz triangular superior, es decir, $A = UTU^*$ donde U es una matriz unitaria y T es una matriz triangular

superior cuya diagonal corresponde a los valores propios de A . Ahora, dado $\epsilon > 0$, existen $(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ tales que para todo $k \in \{1, \dots, n\}$

$$0 \leq \epsilon_k < \frac{\epsilon}{\|U\| \|U^*\|}$$

y los valores $\epsilon_k + \lambda_k$ son distintos. Si D es la matriz diagonal $D = \text{diag}(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$, tenemos que la matriz $T + D$ es diagonalizable pues todos sus valores propios $\epsilon_1 + \lambda_1, \epsilon_2 + \lambda_2, \dots, \epsilon_n + \lambda_n$ son distintos.

La matriz $A_\epsilon = A - UDU^*$ es diagonalizable pues es similar a $T + D$ y para esta matriz se satisface que

$$\|A - A_\epsilon\| = \|UDU^*\| \leq \|U\| \|D\| \|U^*\|$$

donde la última desigualdad se tiene debido a que la norma matricial que viene de una norma vectorial es submultiplicativa. Notemos que

$$\begin{aligned} \|D\| &= \sup\{|Dx| : x \in \mathbb{C}^n \text{ y } |x| = 1\} \\ &= \sup\{|(\epsilon_1 x_1, \dots, \epsilon_n x_n)| : x \in \mathbb{C}^n \text{ y } |x| = 1\} \\ &= \sup\{\sqrt{\epsilon_1^2 x_1^2 + \dots + \epsilon_n^2 x_n^2} : x \in \mathbb{C}^n \text{ y } |x| = 1\} \\ &< \frac{\epsilon}{\|U\| \|U^*\|} \end{aligned}$$

por lo tanto

$$\|A - A_\epsilon\|^2 \leq \|U\| \|D\| \|U^*\| < \frac{\|U\| \epsilon \|U^*\|}{\|U\| \|U^*\|} = \epsilon.$$

Esto implica que el conjunto de matrices diagonalizables es denso en $\mathcal{M}_n(\mathbb{C})$.

Para probar que este resultado no es cierto para matrices con entradas reales consideramos

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad E = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

con $\|E\|_\infty \leq \frac{1}{4}$. En este caso el discriminante de χ_{A+E} es negativo, por lo tanto es posible construir una bola con centro en A que no contenga matrices reales diagonalizables. \square

Proposición 100. El conjunto de matrices diagonalizables de $M_n(\mathbb{R})$ es conexo por caminos.

Demostración. Sean A y B matrices reales diagonalizables. Debemos mostrar que existe una curva, contenida en el espacio de matrices diagonalizables, que tiene a A y a B como puntos extremos.

Definimos tres funciones que van del intervalo $[0, 1]$ en $M_n(\mathbb{R})$. $\gamma_1(t) = (1-t)A$, $\gamma_2(t) = tB$ y

$$\gamma(t) = \begin{cases} \gamma_1(2t) & \text{si } t \in [0, \frac{1}{2}] \\ \gamma_2(2t - 1) & \text{si } t \in [\frac{1}{2}, 1] \end{cases}$$

Notemos que γ_1 y γ_2 son caminos continuos que unen a A y a B , respectivamente, con la matriz nula, además para cada $t \in [0, 1]$ se tiene que $(1-t)A$ y tB son diagonalizables. La función γ es una unión continua de γ_1 y γ_2 , por lo tanto es un camino que tiene a A y a B como puntos extremos y, además, está formado por matrices diagonalizables.

□

2.3.3 Ejercicios

- (i) Demostrar que la intersección de dos topologías sobre X , es una topología.
- (ii) Construir todas las posibles topologías para el conjunto $X = \{a, b, c\}$.
- (iii) Demostrar que la topología punto incluido, definida previamente, es una topología.
- (iv) Demostrar que la norma matricial inducida por la norma euclidiana es submultiplicativa.

2.4 Vocabulario

| | | |
|--------------|------|----------------------|
| Abierto | | Open |
| Arista | | Edge |
| Cerrado | | Closed |
| Compacto | | Compact |
| Conjunto | | Set |
| Demostración | | Proof, demonstration |
| Denso | | Dense |
| Dominio | | Domain |
| Entero | | Integer |
| Enunciado | | Statement |
| Equilátero | | Equilateral |
| Finito | | Finite |
| Grafo | | Graph |
| Impar | | Odd |
| Intersectar | | Intersect |
| Inyectividad | | Injectivity |
| Matriz | | Matrix |
| Mayor que | | Greater than |
| Medida | | Measure |
| Menor que | | Smaller than |
| Norma | | Norm |
| Número primo | | Prime number |
| Par | | Even |
| Segmento | | Segment |
| Topología | | Topology |
| Vector | | Vector |

Bibliografía

- [1] Barnsley, M., *Fractals Everywhere*, segunda edición, Morgan Kaufmann Pub., 1993.
- [2] Fraleigh, J. y Beauregard, R., *Linear Algebra*, tercera edición, Pearson, 1994.
- [3] Johnsonbaugh, R., *Discrete mathematics*, séptima edición. Pearson, 2014.
- [4] Lezama, O., *Cuadernos de Álgebra, Álgebra Lineal.*, Universidad Nacional de Colombia, 2019.
- [5] Munkres, J., *Topology*, segunda edición, Pearson, 2000.
- [6] Omar, M., *Notas de clase, Lecture-Perfect matchings*, Caltech, 2011.
- [7] Rubiano, G., *Topología general*, tercera edición, Universidad Nacional de Colombia, 2010.

Kapitel 3

ToMaTS Deutsch

3.1 Das Schubfachprinzip von Dirichlet

Das sogenannte *Schubfachprinzip* von Johann Peter Gustav Lejeune Dirichlet (1805-1859) aus dem Jahre 1834 wird auf englisch *pigeonhole principle* (Taubenschlagprinzip) genannt. Es lautet wie folgt:

Liegen n Socken in m Schubladen und ist $n > m$, so liegen in mindestens einer Schublade mehr als eine Socke.

3.1.1 Aussage und Beweis

Proposition 101 (Schubfachprinzip von Dirichlet). Seien A und B zwei endliche Mengen und $f : A \rightarrow B$ eine Abbildung. Wir schreiben $n = |A|$ und $m = |B|$.

- (i) Falls $n > m$, so existiert ein $b \in B$ mit $|f^{-1}(\{b\})| \geq 2$.
- (ii) Allgemein, falls $n > rm$ mit $r \in \mathbb{N}$, so existiert ein $b \in B$ mit $|f^{-1}(\{b\})| \geq r + 1$.

Beweis. Es genügt (ii) zu beweisen. Sei $r \in \mathbb{N}$ mit $n > rm$. Wir beweisen die Aussage durch Widerspruch und nehmen an, dass $|f^{-1}(\{b\})| \leq r$ für alle $b \in B$. Es gilt

$$A = \bigsqcup_{b \in B} f^{-1}(\{b\}),$$

und somit

$$n = |A| = \sum_{b \in B} |f^{-1}(\{b\})| \leq r|B| = rm,$$

im Widerspruch zur Annahme. Somit existiert ein $b \in B$ mit $|f^{-1}(\{b\})| \geq r+1$. \square

Bemerkung 102 (Analogie). Der Bezug zur Formulierung mit Socken ist der folgende:

- A ist die Menge der Socken,
- B ist die Menge der Schubladen,
- f ist die Abbildung, welche einer Socke die Schublade zuordnet, in der sie liegt.

Bemerkung 103 (Urbild). Man nennt $f^{-1}(C)$ das *Urbild* der Menge C .

Bemerkung 104 (Injektivität). Anders formuliert, besagt (i), dass keine injektive Abbildung von A nach B existiert falls $|A| > |B|$.

Bemerkung 105 (Zahlen). Wir schreiben $\mathbb{N} := \{0, 1, 2, \dots\}$ für die Menge der natürlichen Zahlen, und $\mathbb{N}^* = \{1, 2, \dots\}$ für die Menge der positiven natürlichen Zahlen.

3.1.2 Leichte Anwendungen

Aus dem Schubfachprinzip lassen sich einige leichte Folgerungen ziehen:

Beispiel 106. In Kopenhagen gibt es mindestens drei Personen, die gleich viele Haare auf dem Kopf haben.

Beweis. Kopenhagen hat mehr als 580.000 Einwohner, und die Anzahl an Haaren jedes Menschen ist nicht grösser als 200.000. Nimmt man somit als Schubfächer die möglichen Anzahlen an Haaren und als Socken die Einwohner von Kopenhagen, so folgt aus dem Schubfachprinzip mit $r = 2$, dass mindestens $2 + 1 = 3$ Einwohner die gleiche Anzahl Haare haben. \square

Beispiel 107 (cf. [15]). Die maximale Anzahl an Königen, die man auf einem Schachbrett so verteilen kann, dass kein König einen anderen König angreift, ist 16.

Beweis. Wir unterteilen das Schachbrett in 16 Quadrate, die jeweils aus vier Feldern bestehen (siehe 3.1). Stehen nun mehr als 16 Könige auf dem Brett, so sind nach dem Schubfachprinzip in mindestens einem der Quadrate zwei Könige. Diese greifen sich notwendigerweise gegenseitig an, somit ist eine solche Stellung nicht zulässig. Umgekehrt existiert aber eine Stellung mit 16 Königen, wie in 3.1 dargestellt. Die Antwort lautet daher 16. \square

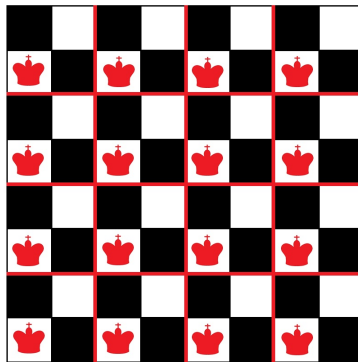


Abbildung 3.1: Schach

Beispiel 108. Wir betrachten 5 Punkte $A_1, \dots, A_5 \in \mathbb{Z}^2$. Zeige, dass für zwei Punkte A_i, A_j der Mittelpunkt $(A_i + A_j)/2$ in \mathbb{Z}^2 liegt.

Beweis. Wir betrachten die Parität der Koordinaten der Punkte A_i und definieren:

$$\begin{aligned} S_{PP} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z}, y \in 2\mathbb{Z}\} \\ S_{PI} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z}, y \in 2\mathbb{Z} + 1\} \\ S_{II} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z} + 1, y \in 2\mathbb{Z} + 1\} \\ S_{IP} &:= \{(x, y) \in \mathbb{Z}^2; x \in 2\mathbb{Z} + 1, y \in 2\mathbb{Z}\}. \end{aligned}$$

Nach dem Schubfachprinzip gibt es zwei Punkte aus A_1, \dots, A_5 , die in der gleichen Menge liegen, sagen wir A_i und A_j . Dann sind beide Koordinaten von $A_i + A_j$ gerade ganze Zahlen, somit liegt $(A_i + A_j)/2$ in \mathbb{Z}^2 . \square

Beispiel 109. Wir platzieren zufällig 5 Punkte auf einer Kugeloberfläche. Dann lässt sich die Kugeloberfläche so in zwei gleichgroße Hälften unterteilen, dass eine der Hälften mindestens 4 der ausgewählten Punkte enthält. Hierbei gehört ein Punkt auf dem trennenden Äquator zu beiden Hälften.

Beweis. Wir wählen zwei der Punkte und betrachten den Äquator, der durch beide Punkte verläuft. Es verbleiben drei Punkte, die sich auf die beiden Hälften verteilen. Nach dem Schubfachprinzip enthält eine der Hälften mindestens zwei der verbliebenen Punkte. Insgesamt enthält diese Hälfte also 4 der 5 Punkte, wie gewünscht. \square

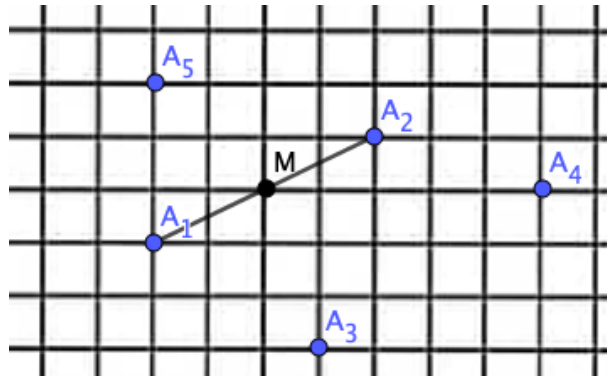


Abbildung 3.2: Jede Menge von fünf Punkten aus \mathbb{Z}^2 enthält ein Paar von Punkten, dessen Mittelpunkt ebenfalls in \mathbb{Z}^2 liegt.

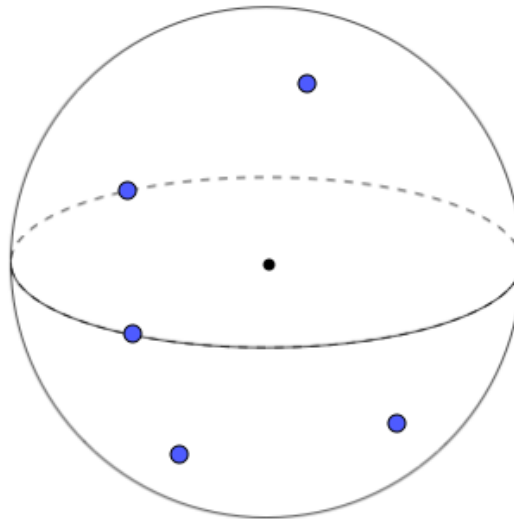


Abbildung 3.3: Fünf Punkte auf einer Kugeloberfläche.

Beispiel 110 (Die Ramsey-Zahl). Auf einem Fest mit (mindestens) 6 Personen gibt es stets drei Personen, die sich kennen, oder drei Personen, die sich nicht kennen.

Beweis. Wir wählen 6 Punkte $x_1, \dots, x_6 \in \mathbb{R}^2$ in der Ebene, korrespondierend zu den 6 Personen. Falls zwei Personen sich kennen, zeichnen wir eine blaue Gerade zwischen den entsprechenden Punkten, falls sie sich nicht kennen, eine grüne. Von der Person x_1 gehen also 5 Geraden aus mit höchstens zwei verschiedenen Farben. Nach dem Schubfachprinzip (angewandt mit $n = 5$, $m = 2$ und $r = 2$) gibt es also mindestens 3 Geraden gleicher Farbe. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass die Punkte auf der anderen Seite der Geraden x_2, x_3

und x_4 sind und dass die Farbe blau ist. Es gibt nun zwei Möglichkeiten:

- Eine der Geraden $[x_2, x_3]$, $[x_3, x_4]$ und $[x_2, x_4]$ ist blau. Dann erhalten wir ein blaues Dreieck, was bedeutet, dass sich drei Personen kennen.
- Keine dieser drei Geraden ist blau. Demnach ist das Dreieck $x_2x_3x_4$ grün, und somit kennen sich die entsprechenden drei Personen nicht.

In jedem Fall ist die Aussage bewiesen. \square

Beispiel 111 (Mathematikwettbewerb der Klassen 4-7, Regalia 6, Sofia (1993). cf. [3]). Seien ABC ein gleichseitiges Dreieck und $MNPQ$ ein Quadrat, deren Eckpunkte auf einem Kreis vom Umfang s liegen und paarweise verschieden sind (siehe 3.4). Die 7 Punkte teilen den Kreis also in 7 Bögen. Dann hat mindestens einer dieser Bögen eine Länge kürzer als $s/24$.

Beweis. Die Eckpunkte des Dreiecks teilen den Kreis in 3 Bögen und das Quadrat hat 4 Eckpunkte, somit gibt es nach dem Schubfachprinzip zwei Eckpunkte des Dreiecks zwischen denen mindestens zwei Eckpunkte des Quadrats liegen. Angenommen die Punkte M und N liegen auf dem Bogen \widehat{AB} . Schreiben wir $\ell(XY)$ für die Länge des Bogens \widehat{XY} , so gilt

$$\ell(AB) = \frac{s}{3} \quad \text{und} \quad \ell(MN) = \frac{s}{4},$$

und somit

$$\ell(AM) + \ell(NB) = \frac{s}{3} - \frac{s}{4} = \frac{s}{12}.$$

Folglich hat einer der Bögen \widehat{AM} und \widehat{NB} eine Länge kürzer als $s/24$. \square

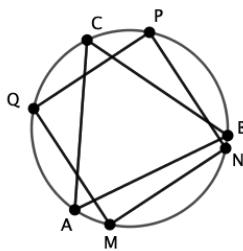


Abbildung 3.4: Skizze zu 111

Beispiel 112 (Ein Resultat von Vázsonyi und Sved. Siehe [2]). Seien a_1, \dots, a_n ganze Zahlen, nicht notwendigerweise verschieden. Dann gibt es natürliche Zahlen $0 \leq k < \ell \leq n$ für die gilt, dass die Summe $\sum_{i=k+1}^{\ell} a_i$ ein Vielfaches von n ist.

Beweis. Seien

$$A = \{(0, 0), (1, a_1), (2, a_1 + a_2), \dots, (n, a_1 + a_2 + \dots + a_n)\}$$

und $B = \{0, 1, \dots, n-1\}$. Wir betrachten die Abbildung $f : A \rightarrow B$ welche (i, m) auf den Rest nach Division von m durch n schickt. Da $|A| = n+1 > n = |B|$, existieren zwei Summen $a_1 + \dots + a_k$ und $a_1 + \dots + a_\ell$ (mit $k < \ell$) deren Rest nach Division durch n der gleiche ist. Es folgt, dass

$$\sum_{i=k+1}^{\ell} a_i = \sum_{i=1}^{\ell} a_i - \sum_{i=1}^k a_i$$

durch n teilbar ist, was die Aussage beweist. \square

Das Schubfachprinzip lässt sich auch auf Abbildungen zwischen unendlichen Mengen verallgemeinern. Das folgende Beispiel ist eine Anwendung dieses Schubfachprinzips für unendliche Mengen.

Beispiel 113 (Ein „unendliches“ Schubfachprinzip). Für alle $c \in \mathbb{Q}_+^* \setminus \{1\}$ existieren $a, b \in \mathbb{R} \setminus \mathbb{Q}$, die die Gleichung $c = a^b$ erfüllen.

Beweis. Sei $c \in \mathbb{Q}_+^* \setminus \{1\}$. Wir betrachten die Abbildung

$$f_c : \mathbb{R}_{>0} \setminus \{1\} \rightarrow \mathbb{R}, a \mapsto \frac{\ln(c)}{\ln(a)}$$

welche jedem $a > 0$ die Lösung $b = \frac{\ln(c)}{\ln(a)}$ der Gleichung $a^b = c$ zuweist (welche existiert, da a größer als 0, aber nicht 1 ist und somit $\ln(a) \in \mathbb{R}^*$). Diese Funktion ist injektiv, da $\ln : \mathbb{R}_{>0} \setminus \{1\} \rightarrow \mathbb{R}^*$ injektiv ist. Beschränkt man diese Abbildung auf die positiven irrationalen Zahlen und nimmt an es gäbe keine Lösungen $a, b \in \mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$ der Gleichung $a^b = c$, so folgt, dass $f_c : \mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty) \rightarrow \mathbb{Q}$ eine injektive Abbildung in die rationalen Zahlen ist. Aber die Kardinalität von $\mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$ ist größer als die von \mathbb{Q} , da \mathbb{Q} abzählbar ist und $\mathbb{R} \setminus \mathbb{Q} \cap (0, +\infty)$ nicht. Somit erhält man einen Widerspruch und die Aussage ist bewiesen. \square

3.1.3 Dirichlets Approximationssatz

Nun kommen wir zu einem anspruchsvolleren mathematischen Satz, welcher mit dem Schubfachprinzip bewiesen werden kann. Er handelt davon, wie gut sich irrationale Zahlen durch rationale Zahlen mit möglichst kleinem Nenner approximieren lassen. Die folgenden zwei Abschnitte sind aus [6].

Aussage und Beweis des Satzes

Satz 114 (Dirichlet). Sei α eine irrationale Zahl und N eine positive natürliche Zahl. Dann gibt es eine rationale Zahl $\frac{p}{q}$, deren Nenner q zwischen 1 und N liegt, und für die

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN}$$

gilt.

Beweis. Die Ungleichung $\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN}$ lässt sich auch so ausdrücken, dass $\alpha \cdot q$ weniger als $\frac{1}{N}$ von einer ganzen Zahl p entfernt ist. Also möchten wir zeigen, dass es ein q zwischen 1 und N gibt, derart, dass $\alpha \cdot q$ weniger als $\frac{1}{N}$ von einer ganzen Zahl entfernt liegt.

Als Schubfächer verwenden wir die N halboffenen Intervalle

$$\left[0, \frac{1}{N} \right), \left[\frac{1}{N}, \frac{2}{N} \right), \dots, \left[\frac{N-1}{N}, 1 \right).$$

Um die Objekte zu definieren, benötigen wir den „Bruchanteil“ einer reellen Zahl x , welcher definiert ist als der Teil der Dezimaldarstellung, der hinter dem Komma kommt und welchen wir mit $\langle x \rangle$ bezeichnen. Genauer definieren wir zunächst für eine reelle Zahl x die ganze Zahl $[x]$ als die grösste ganze Zahl, die kleiner oder gleich x ist, und dann $\langle x \rangle = x - [x]$. Zum Beispiel ist $\langle 13,27234678\dots \rangle = 0,27234678\dots$. Der Bruchanteil liegt stets in $[0, 1)$. Als Objekte nehmen wir nun die $N+1$ Zahlen $0, \langle \alpha \rangle, \langle \alpha \cdot 2 \rangle, \dots, \langle \alpha \cdot N \rangle$. Nach dem Schubfachprinzip liegen also zwei dieser Zahlen im gleichen Intervall, sagen wir $\langle \alpha \cdot r \rangle$ und $\langle \alpha \cdot s \rangle$, mit $r > s$. Aber dann ist die Differenz $\alpha \cdot (r - s)$ weniger als $\frac{1}{N}$ von einer ganzen Zahl entfernt. Da ausserdem $1 \leq r - s \leq N$ gilt, ist der Beweis abgeschlossen. \square

Kriterium für Irrationalität

In diesem Abschnitt diskutieren wir ein Kriterium für die Irrationalität reeller Zahlen, welches sich aus dem Satz des vorherigen Abschnitts ergibt.

Proposition 115. Eine Zahl $\alpha \in \mathbb{R}$ ist genau dann irrational, wenn zwei Folgen ganzer Zahlen $(p_n)_{n \in \mathbb{N}^*}$ und $(q_n)_{n \in \mathbb{N}^*}$ existieren mit der Eigenschaft, dass

$$\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$$

und $q_n \alpha - p_n \neq 0$ für alle n .

Beweis. Angenommen α ist irrational. Nach Satz 114 existieren für alle $n \in \mathbb{N}^*$ ganze Zahlen p_n und q_n derart, dass $1 \leq q_n \leq n$ und

$$|q_n \alpha - p_n| \leq \frac{1}{n}.$$

Es folgt, dass $\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$. Ausserdem ist stets $q_n \alpha - p_n \neq 0$, da α irrational ist.

Umgekehrt nehmen wir nun an es existieren Folgen $(p_n)_{n \in \mathbb{N}^*}$ und $(q_n)_{n \in \mathbb{N}^*}$ derart, dass

$$\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$$

und $q_n \alpha - p_n \neq 0$ für alle $n \in \mathbb{N}^*$. Wir beweisen per Widerspruch und nehmen an, dass α in \mathbb{Q} liegt und sich schreiben lässt als $\alpha = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$ und $b > 0$. Es folgt, dass

$$|q_n \alpha - p_n| = \left| \frac{q_n a - p_n b}{b} \right| \geq \frac{1}{b},$$

da $q_n \alpha - p_n \neq 0$ für alle n . Dies widerspricht der Annahme, dass $\lim_{n \rightarrow +\infty} q_n \alpha - p_n = 0$, und somit muss α irrational sein. \square

Hiermit lässt sich schnell sehen:

Korollar 116. Die Zahl $\sqrt{2}$ ist irrational.

Beweis. Faktorisiert man den Ausdruck $(\sqrt{2} - 1)^n$ aus, so erhält man für alle $n \in \mathbb{N}$, dass

$$(\sqrt{2} - 1)^n = q_n \sqrt{2} - p_n,$$

mit $p_n, q_n \in \mathbb{Z}$. Es ist

$$\lim_{n \rightarrow +\infty} q_n \sqrt{2} - p_n = \lim_{n \rightarrow +\infty} (\sqrt{2} - 1)^n = 0,$$

da $|\sqrt{2} - 1| < 1$. Ausserdem gilt

$$q_n \sqrt{2} - p_n = (\sqrt{2} - 1)^n \neq 0$$

für alle $n \in \mathbb{N}$, da $\sqrt{2} \neq 1$. Nach Proposition 115 ist $\sqrt{2}$ demnach irrational. \square

Divergente Reihen

In diesem Abschnitt demonstrieren wir, inspiriert durch [17, 14], wie Dirichlets Approximationssatz dazu benutzt werden kann zu zeigen, dass eine Reihe divergiert. Wir beginnen mit folgendem Lemma:

Lemma 117. Sei α irrational. Dann existieren unendlich viele Paare ganzer Zahlen (p, q) , $q > 0$ für die die Ungleichung

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

gilt.

Beweis. Nach Satz 114 wissen wir, dass für alle $N \in \mathbb{N}^*$ Zahlen $q \in \{1, \dots, N\}$ und $p \in \mathbb{Z}$ existieren derart, dass

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

Wir zeigen nun, dass die Menge C der Paare (p, q) , die diese Eigenschaft erfüllen, sogar unendlich ist. Wir nehmen an es wären nur endlich viele $C = \{(p_i, q_i)\}_{1 \leq i \leq r}$ und leiten einen Widerspruch her. Wir definieren

$$\epsilon := \min_i \left\{ \left| \alpha - \frac{p_i}{q_i} \right| \right\}.$$

Da $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, folgt $\epsilon > 0$. Dann existiert ein $N_0 > 0$ mit $\epsilon > \frac{1}{N_0}$. Wendet man nun Satz 114 auf die Zahl N_0 und α an, so existiert ein Paar (p_0, q_0) mit

$$\left| \alpha - \frac{p_0}{q_0} \right| < \frac{1}{N_0 q_0}$$

Es folgt wie oben, dass $\left| \alpha - \frac{p_0}{q_0} \right| < \frac{1}{q_0^2}$, sodass (p_0, q_0) in C liegen muss. Andererseits folgt aber auch

$$\left| \alpha - \frac{p_0}{q_0} \right| < \frac{1}{N_0 q_0} \leq \frac{1}{N_0} < \epsilon$$

im Widerspruch zur Definition von ϵ . □

Proposition 118. Die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^2 \sin^2(n)}$ ist divergent.

Beweis. Da π irrational ist, existieren nach Lemma 117 unendliche viele Paare natürlicher Zahlen n, q mit

$$\left| \pi - \frac{n}{q} \right| < \frac{1}{q^2}.$$

Dies impliziert, dass es unendlich viele n, q gibt mit $\pi - n/q > -1/q^2$. Weil $q \geq 1$, gibt es somit unendlich viele Paare n, q mit

$$\frac{n}{q} < \pi + \frac{1}{q^2} \leq \pi + 1.$$

Es folgt, dass für alle solchen n, q die Ungleichung

$$|\sin(n)| = |\sin(n - q\pi)| \leq |n - q\pi| < \frac{1}{q} = \frac{1}{n} \frac{n}{q} < \frac{\pi + 1}{n}$$

gilt. Demnach existieren unendlich viele natürliche Zahlen n mit

$$\frac{1}{n^2 \sin^2(n)} > \frac{1}{(1 + \pi)^2}.$$

Folglich divergiert die Reihe über die Werte $\frac{1}{n^2 \sin^2(n)}$. □

3.2 Eulers Formel

Einige der Resultate in diesem Kapitel sind angelehnt an [2] und [12].

3.2.1 Die Euler-Formel und planare Graphen

Wir benötigen zunächst einige Begriffe aus der Graphentheorie:

Definition 119.

- Ein (ungerichteter) *Graph* $G = (V, E)$ besteht aus einer Menge von *Knoten* V , einer Menge von *Kanten* E , sowie einer Funktion von E in die Menge $(V \times V)/\Sigma_2$ der ungeordneten Paare (v_1, v_2) von Elementen aus V , welche ausdrückt welche beiden Knoten von einer Kante verbunden werden.

Ein Graph ist

- *planar*, wenn er sich in die Ebene \mathbb{R}^2 einbetten lässt, ohne dass sich Kanten überschneiden. Eine solche Einbettung zerlegt demnach die Ebene in eine Anzahl Flächen, wovon eine aus dem unbegrenzten äusseren Teil besteht. Die Menge dieser Flächen bezeichnen wir mit F .
- *zusammenhängend*, wenn für jedes Paar von verschiedenen Knoten (x, y) eine Folge von Kanten existiert, die x mit y verbindet.
- *einfach*, wenn er keine Schleifen (d.h., Kanten, die einen Knoten mit sich selbst verbinden) oder Doppelkanten enthält.
- *kreisfrei*, wenn es keine Wege (die jede Kante maximal einmal, aber mindestens eine Kante enthalten) mit gleichem Start- und Endknoten gibt.
- *leer*, falls V und E die leere Menge sind.

- Mit $|V|$, $|E|$ und $|F|$ bezeichnen wir die Anzahl der Knoten, Kanten bzw. Flächen.
- Ein *Baum* ist ein zusammenhängender und kreisfreier Graph.

Lemma 120. Sei $G = (V, E)$ ein nichtleerer Baum. Dann ist $|V| = |E| + 1$.

Beweis. Wir beweisen per Induktion über $|E|$: Falls G keine Kante hat, so muss G mindestens einen Knoten haben, da G nicht leer ist. Da G zusammenhängend ist gibt es allerdings auch nicht mehr als einen Knoten. Nehmen wir nun an, dass $n > 1$ ist und die Aussage für $|E| < n$ schon bewiesen wurde. Sei G ein nichtleerer Baum mit $|E| = n$. Sei $e \in E$ eine beliebige Kante. Entfernen wir diese Kante, so zerfällt der verbleibende Graph in zwei Zusammenhangskomponenten, da G ansonsten einen Kreis gehabt hätte. Beide Komponenten sind dann nichtleere Bäume mit weniger als n Kanten, sodass sich die Induktionshypothese anwenden lässt. \square

Satz 121. Ist $G = (V, E)$ ein nichtleerer, einfacher und zusammenhängender planarer Graph, so gilt für jede Einbettung

$$|V| - |E| + |F| = 2.$$

Insbesondere ist $|F|$ unabhängig von der Einbettung.

Beweis. Wir beweisen die Aussage per Induktion über $|E|$. Für den Induktionsanfang bemerken wir, dass im Fall $|E| = 0$ der Graph nur zusammenhängend sein kann, falls $|V| = 1$ ist und dann auch $|F| = 1$ gilt.

Für den Induktionsschritt nehmen wir nun an, dass die Aussage schon für alle Graphen mit weniger Kanten bewiesen wurde. Wir machen eine Fallunterscheidung.

Fall 1: G ist kreisfrei

Als kreisfreier zusammenhängender Graph ist G ein Baum. In diesem Fall gibt es keine beschränkte Fläche und somit ist $|F| = 1$. Damit folgt die Aussage aus Lemma 120.

Fall 2: G ist nicht kreisfrei

Sei e eine Kante von G , die in einem Kreis liegt. Die beiden Endknoten von e sind also über einen Weg verbunden, der nicht über e geht, sodass $G \setminus e$ noch immer zusammenhängend ist. $G \setminus e$ hat sowohl eine Kante als auch eine Fläche weniger als G , da die beiden Flächen auf den zwei Seiten von e zu einer Fläche werden (es waren vorher zwei verschiedene Flächen, da e Teil eines Kreises war). Die Aussage folgt nun direkt aus der Induktionsvoraussetzung. \square

3.2.2 Platonische Körper und Parkettierungen der Sphäre

Entfernen wir einen Punkt von der (2-)Sphäre, so ist der Rest mittels der stereographischen Projektion zur Ebene äquivalent. Fragen über konvexe Polyeder lassen sich so zu Fragen über planare Graphen übertragen. Genauergesagt wählt man für den Übergang eine Seitenfläche des Polyeders, an die keine dazu parallele Seitenfläche angrenzt (der Einfachheit halber gehen wir hier von dem regulären Fall aus, dass eine solche existiert). Dann hebt man einen gewählten Punkt x im Inneren dieser Fläche um einen kleinen Betrag an, derart dass das neue Polyeder, das von den vorherigen Eckpunkten sowie dem neuen aufgespannt wird weiterhin konvex bleibt. Nun kann man das (ursprüngliche) Polyeder von dem angehobenen Punkt x aus stereographisch auf eine Ebene auf der anderen Seite des Polyeders projizieren, und dies überführt die Kanten des Polyeders in Kanten in der Ebene welche sich aufgrund der Konvexität nicht überschneiden. Folglich erhält man einen planaren Graphen.

Eine erste Anwendung der Eulerschen Formel auf Polyeder dieser Art ist der folgende Satz:

Proposition 122. Jedes konvexe Polyeder bei dem jeder Eckpunkt Teil genau dreier Polygone ist, und welches nur aus Fünf- und Sechsecken besteht, hat genau 12 Fünfecke.

Beweis. Sei P die Zahl der Fünfecke und H die Zahl der Sechsecke. Die Gesamtzahl der Seiten des Polyeders ist also

$$|F| = P + H.$$

Da jeder Eckpunkt Teil von drei Polygonen ist, und jede Kante an genau zwei Polygonen angrenzt, erhält man

$$|V| = \frac{5P + 6H}{3}, \quad |E| = \frac{5P + 6H}{2}.$$

Daraus ergibt sich $|V| - |E| + |F| = \frac{P}{6}$, und nach der Eulerschen Formel (welche anwendbar ist aufgrund der angenommenen Konvexität) folgt $P = 12$. \square

Definition 123. Ein Polyeder heisst *regulär*, wenn all seine Seiten zu dem gleichen regelmässigen Polygon identisch sind und an jedem Eckpunkt die gleiche Anzahl Seiten angrenzen. Ein regulärer und konvexer Polyeder wird *platonischer Körper* genannt.

Satz 124. Es gibt genau 5 platonische Körper:

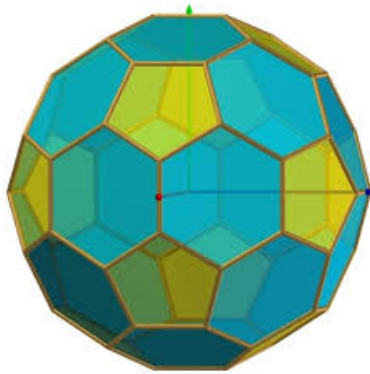


Abbildung 3.5: Polyeder bestehend aus Fünf- und Sechsecken

- Das Tetraeder (besteht aus 4 Dreiecken),
- den Würfel (besteht aus 6 Quadraten),
- das Oktaeder (besteht aus 8 Dreiecken),
- das Dodekaeder (besteht aus 12 Fünfecken), und
- das Ikosaeder (besteht aus 20 Dreiecken).

Beweis. Wir beweisen hier nur, dass es maximal die angegebenen platonischen Körper geben kann - für einen vollständigen Beweis müsste noch zusätzlich gezeigt werden, dass diese platonischen Körper tatsächlich existieren.

Sei also S ein platonischer Körper mit n Ecken, a Kanten und f Flächen, mit $k \geq 3$ Kanten pro Fläche und $d \geq 3$ Kanten pro Eckpunkt. Es gilt:

- (i) Da jede Kante an zwei Flächen grenzt, ist $kf = 2a$,
- (ii) Da jede Kante zwei Ecken hat, ist $dn = 2a$.

Weiterhin besagt die Eulersche Formel, dass

$$n - a + f = 2.$$

Ersetzt man nun n und f durch $2a/d$ und $2a/k$, so ergibt sich

$$\frac{2a}{d} - a + \frac{2a}{k} = 2.$$

Nach Teilen durch $2a$ erhält man

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{a} + \frac{1}{2}.$$

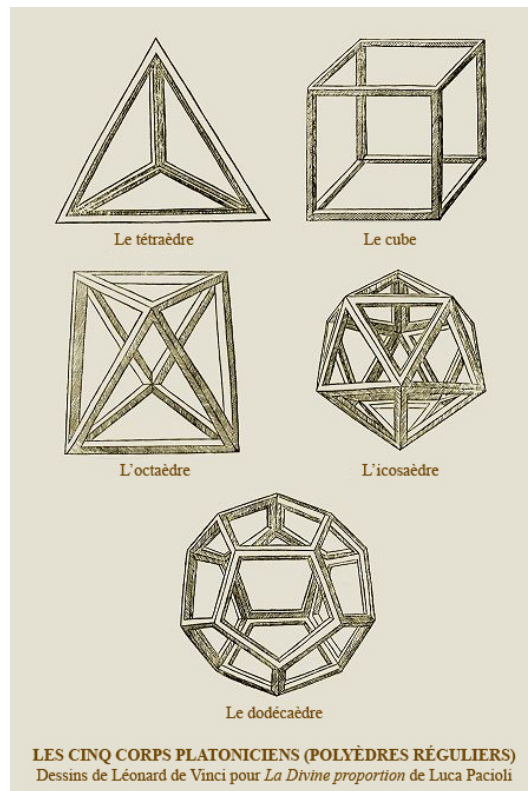


Abbildung 3.6: Die platonischen Körper

Wir werden nun zeigen, dass diese Gleichungen nur fünf ganzzahlige Lösungen mit $d \geq 3, k \geq 3, a \geq 1$ zulässt. Man bemerke, dass für eine Lösung insbesondere $\frac{1}{k} + \frac{1}{d} > \frac{1}{2}$ gilt.

Fall 1 : Ist $d \geq 6$, so ist $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{6} + \frac{1}{3} \leq \frac{1}{2}$, demnach gibt es keine solche Lösung.

Fall 2 : Sei $d = 5$. Für $k = 3$ hat die Gleichung eine Lösung mit $a = 30$, dargestellt durch das Ikosaeder. Ist $k \geq 4$, so folgt $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ und die Gleichung lässt keine Lösung zu.

Fall 3 : Sei $d = 4$. Erneut gibt es eine Lösung mit $k = 3$ und $a = 12$, dargestellt durch das Oktaeder. Ist $k \geq 4$, so folgt erneut $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ und demnach existiert keine weitere Lösung.

Fall 4 : Sei $d = 3$. Dann existieren folgende Lösungen:

- $k = 3$ und $a = 6$ (Tetraeder),
- $k = 4$ und $a = 12$ (Würfel),

- $k = 5$ und $a = 30$ (Dodekaeder).

Ist aber $k \geq 6$, so folgt $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ und es existiert keine weitere Lösung. \square

3.2.3 Der Satz von Pick

In diesem Abschnitt erklären wir eine zur eulerschen Formel äquivalente Aussage, den Satz von Pick. Wir beginnen mit:

Proposition 125. Seien $p_1, p_2 \in \mathbb{Z}^2$ verschieden, und so, dass das von $0, p_1$ und p_2 aufgespannte Dreieck Δ keine weiteren Punkte aus \mathbb{Z}^2 enthält (weder im Inneren, noch auf dem Rand). Dann gilt für den Flächeninhalt des Dreiecks $A(\Delta) = \frac{1}{2}$.

Beweis.

Schritt 1: Reduktion auf $A(P)$: Wir betrachten jetzt die Punktspiegelung an dem Punkt $(p_1 + p_2)/2$. Diese ist durch die Formel $\sigma: x \mapsto p_1 + p_2 - x$ gegeben und bildet das Dreieck Δ auf ein weiteres Dreieck $\sigma(\Delta)$ ab. Der Schnitt der beiden Dreiecke besteht genau aus der gemeinsamen Kante von p_1 bis p_2 , und die Vereinigung $\Delta \cup \sigma(\Delta)$ ist das von p_1 und p_1 aufgespannte Parallelogramm, welches wir P nennen. Es ist also $A(\Delta) = A(P)/2$, sodass es genügt zu zeigen, dass $A(P) = 1$. Da $(p_1 + p_2)/2$ nur halbganzzahlige Komponenten hat, bildet die Punktspiegelung σ das Gitter \mathbb{Z}^2 auf \mathbb{Z}^2 ab. Folglich beinhaltet P bis auf $0, p_1, p_2$ und $p_1 + p_2$ keine weiteren Gitterpunkte.

Schritt 2: Parkettierung der Ebene: Durch Verschiebungen von P entlang $\mathbb{Z}p_1 + \mathbb{Z}p_2$ erhalten wir eine Parkettierung der Ebene. Da p_1 und p_2 ganzzahlige Komponenten haben und P das Gitter \mathbb{Z}^2 genau in den Eckpunkten schneidet, gilt dies ebenfalls für Verschiebungen von P . Folglich sind die Eckpunkte der Parkettierung genau \mathbb{Z}^2 .

Schritt 3: Definitionen: Sei S das Quadrat $[0, n] \times [0, n]$ und sei Q_n die Fläche, die aus allen Parallelogrammen der Parkettierung der Ebene aus Schritt 2 gebildet wird, die S schneiden. Wir definieren weiterhin:

- Sei p_n die Anzahl der Parallelogramme, die Teil von Q_n sind.
- Sei v_Q die Anzahl der Punkte von \mathbb{Z}^2 , die in Q_n liegen, aber nicht in S .
- Sei v_S die Anzahl der Punkte von \mathbb{Z}^2 , die in S liegen.
- Sei x (bzw. y) die Differenz zwischen dem Maximum und Minimum, den die Projektion auf die erste (bzw. zweite) Koordinate auf P annimmt.
- Sei z das Maximum von x und y .

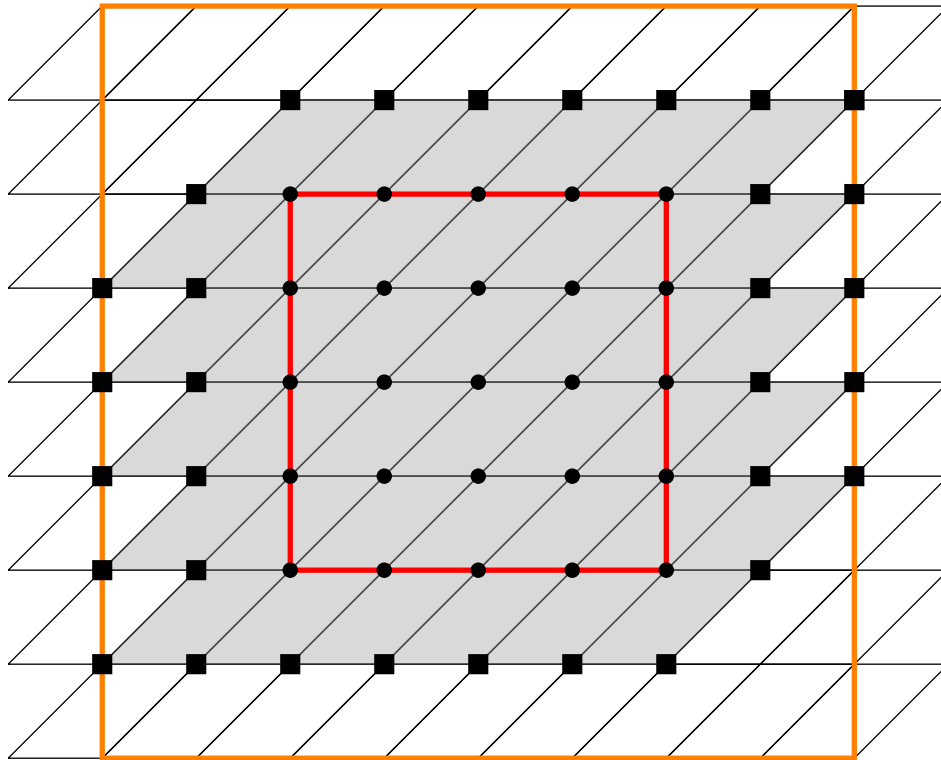


Abbildung 3.7: Skizze zu den Definitionen in Schritt 3 im Beweis von Proposition 125: Das Parallelogramm in diesem Beispiel wird von $p_1 = (1, 0)$ und $p_2 = (1, 1)$ aufgespannt. Es gilt dann $x = 2, y = 1$ und $z = 2$. Das zu $n = 4$ zugehörige S wird durch das rote Quadrat dargestellt, das Quadrat $[-z, n+z] \times [-z, n+z]$ wird durch das orangene Quadrat dargestellt, und die Fläche Q_n ist hellgrau gefärbt. Wir erhalten $p_n = 40$, $v_Q = 32$ (Punkte mit Quadraten markiert), und $v_S = 25$ (Punkte mit Kreisen markiert).

Figure 3.7 enthält eine Skizze zu diesen Definitionen.

Schritt 4: Abschätzungen für $A(Q_n)$: Per Definition gilt $S \subseteq Q_n$ und damit $n^2 = A(S) \leq A(Q_n)$. Da jede Verschiebung von P , die Teil von Q_n ist, nicht-leeren Schnitt mit S haben muss, kann die Entfernung der Eckpunkte dieses Parallelogramms von S maximal z betragen. Es folgt, dass $Q_n \subseteq [-z, n+z] \times [-z, n+z]$. Also ist $A(Q_n) \leq (n + 2z)^2$.

Schritt 5: Abschätzungen für p_n : Wir schätzen p_n ab indem wir Eckpunkte zählen. Jedes Parallelogramm hat vier Eckpunkte. Wir zählen also $4p_n$ Eckpunkte. Allerdings haben wir damit Eckpunkte, an die mehrere Parallelogramme aus Q_n anliegen, mehrfach gezählt. Jeder Eckpunkt in S hat genau vier anliegende Paral-

lelogramme, und Ecken ausserhalb von S mindestens eines. Wir erhalten damit:

$$4p_n \geq 4v_S + v_Q \geq 4(n+1)^2 + 0 = 4n^2 + 8n + 4$$

Es folgt $p_n \geq n^2$.

Für die Abschätzung nach oben nutzen wir, dass jeder Eckpunkt an maximal vier Parallelogrammen anliegen kann. Also ist $4p_n \leq 4(v_S + v_Q)$ und damit

$$p_n \leq v_S + v_Q.$$

Da wie in Schritt 4 bemerkt $Q_n \subseteq [-z, n+z] \times [-z, n+z]$, gilt insbesondere, dass $v_S + v_Q$ kleiner oder gleich der Anzahl an Punkten in $[-z, n+z] \times [-z, n+z] \cap \mathbb{Z}^2$ ist. Es folgt also

$$p_n \leq (n+2z+1)^2 = n^2 + 4nz + 2n + 4z^2 + 4z + 1$$

Schritt 6: Formel für $A(P)$: Da alle Parallelogramme in Q_n Verschiebungen von P sind und sich nur in Kanten schneiden, gilt für den Flächeninhalt: $A(Q_n) = A(P) \cdot p_n$. Folglich ist $A(P) = A(Q_n)/p_n$ für jedes n und für den Grenzwert gilt also:

$$A(P) = \lim_{n \rightarrow \infty} \frac{A(Q_n)}{p_n}$$

Schritt 7: Abschätzung des Grenzwertes nach oben: Wir nutzen jetzt die Abschätzung von $A(Q_n)$ nach oben aus Schritt 4 und die Abschätzung von p_n nach unten aus Schritt 5:

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{A(Q_n)}{p_n} &\leq \lim_{n \rightarrow \infty} \frac{(n+2z)^2}{n^2} = \lim_{n \rightarrow \infty} \frac{n^2 + 4nz + 4z^2}{n^2} \\ &= \lim_{n \rightarrow \infty} 1 + \frac{4z}{n} + \frac{4z^2}{n^2} = 1 \end{aligned}$$

Schritt 8: Abschätzung des Grenzwertes nach unten: Wir nutzen jetzt die Abschätzung von $A(Q_n)$ nach unten aus Schritt 4 und die Abschätzung von p_n nach oben aus Schritt 5:

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{A(Q_n)}{p_n} &\geq \lim_{n \rightarrow \infty} \frac{n^2}{n^2 + 4nz + 2n + 4z^2 + 4z + 1} \\ &= \lim_{n \rightarrow \infty} \frac{1}{1 + \frac{4z+2}{n} + \frac{4z^2+4z+1}{n^2}} \\ &= \frac{\lim_{n \rightarrow \infty} 1}{\lim_{n \rightarrow \infty} 1 + \frac{4z+2}{n} + \frac{4z^2+4z+1}{n^2}} = \frac{1}{1} = 1 \end{aligned}$$

Schritt 9: Flächeninhalt von P : Es folgt aus Schritten 6, 7 und 8, dass $1 \leq A(P) \leq 1$ und somit $A(P) = 1$. \square

Bemerkung 126. Im obigen Beweis haben wir (fast) gezeigt, dass genau dann, wenn das aufgespannte Dreieck keine weiteren Punkte aus \mathbb{Z}^2 enthält, \mathbb{Z}^2 die Menge der Eckpunkte der durch P erhaltenen Parkettierung der Ebene ist. Dies wiederum ist äquivalent dazu, dass (p_1, p_2) die abelsche Gruppe \mathbb{Z}^2 erzeugt, was äquivalent dazu ist, dass (p_1, p_2) eine Basis von \mathbb{Z}^2 ist.

Wir benötigen folgendes Ergebnis für den Beweis des Satzes von Pick:

Proposition 127. Sei P ein einfaches Polygon mit mehr als drei Eckpunkten. Dann gibt es eine Diagonale (d.h. Strecke zwischen zwei Eckpunkten), die den Streckenzug von P nur in den beiden Endpunkten schneidet.

Beweis. Siehe zu diesem Beweis auch die Skizze in Figure 3.8. Der Beweis basiert auf dem Beweis einer stärkeren Aussage in [11]. Sei v_m ein solcher Eckpunkt von P , mit angrenzenden Eckpunkten v_a und v_b , dass der Innenwinkel $\angle v_b v_m v_a$ kleiner als 180° ist. Wir unterscheiden zwei Fälle: Falls die Strecke von v_a nach v_b die Kanten von P ausserhalb von v_a und v_b nicht schneidet, so sind wir fertig. Nehmen wir nun also an, dass dies nicht der Fall ist. Da P mehr als drei Eckpunkte hat muss es dann Eckpunkte ausser v_a, v_m und v_b geben, die in dem von diesen drei Punkten aufgespannten Dreieck liegen. Sei z eines dieser Eckpunkte mit der Eigenschaft, dass die zu $v_a v_b$ parallele Gerade durch z minimalen Abstand von v_m hat. Es folgt, dass die Strecke $[v_m z]$ die Kanten von P nur in v_m und z schneidet. Folglich ist $[v_m z]$ die gesuchte Diagonale. \square

Satz 128 (Satz von Pick). Die Fläche $A(P)$ eines (einfachen¹) Polygons $P \subset \mathbb{R}^2$ mit Eckpunkten in \mathbb{Z}^2 beträgt

$$A(P) = n_i + \frac{n_b}{2} - 1,$$

wobei n_i die Anzahl der \mathbb{Z}^2 -Gitterpunkte im Inneren des Polygons Q bezeichnet, und n_b die Anzahl der \mathbb{Z}^2 -Gitterpunkte auf dem Rand.

Beweis. Sei m die Anzahl der Eckpunkte von P . Wir beweisen per doppelter Induktion, zunächst über m , dann über $n_b/2 + n_i$.

Fall $m = 3, n_b/2 + n_i = 3/2$: In diesem Fall ist dies exakt die Aussage von Proposition 125, da $n_b = 3$ und daher auch $n_i = 0$ sein muss.

Fall $m = 3, n_b/2 + n_i > 3/2, n_i > 0$: Sei Z einer der inneren Gitterpunkte und seien A, B, C die Eckpunkte von P . Dann liegen die Strecken von Z zu A, B bzw. C vollständig in P und teilen die Fläche des Dreiecks P in drei Dreiecke. Seien n_i^{ABZ} , n_i^{CAZ} und n_i^{BCZ} die jeweilige Anzahl der inneren Gitterpunkte der Dreiecke

¹d.h. Kanten schneiden sich nur in den Eckpunkten

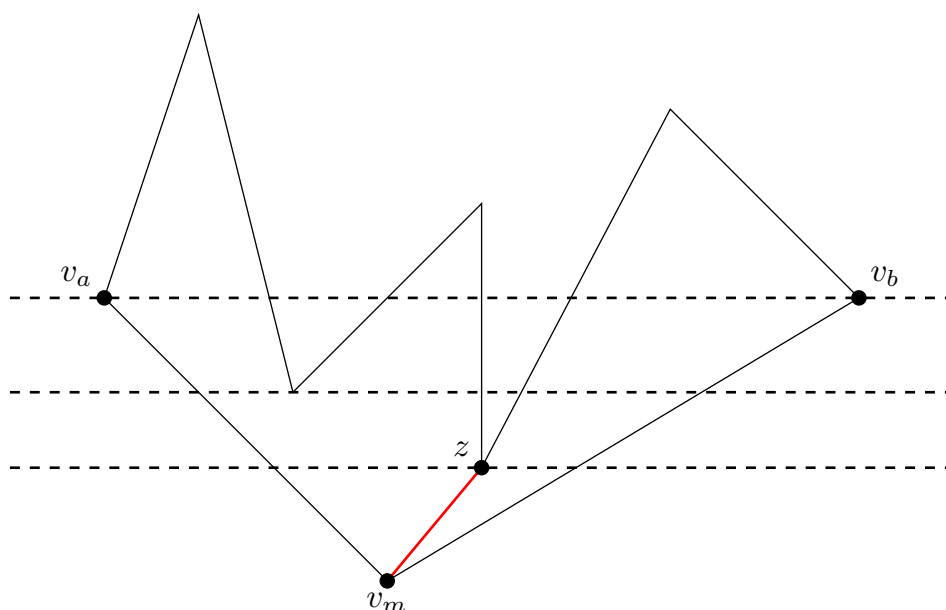


Abbildung 3.8: Skizze zu Proposition 127

$\triangle ABZ$, $\triangle CAZ$ bzw. $\triangle BCZ$, und b_A , b_B bzw. b_C die Anzahl der Gitterpunkte die im Inneren der Strecke AZ , BZ bzw. CZ liegen. Seien k_{AB} , k_{BC} und k_{CA} die Anzahl der Gitterpunkte die im Inneren der Kanten AB , BC bzw. CA liegen. Sei n_b^{ABZ} die Anzahl der Gitterpunkte auf dem Rand des Dreiecks $\triangle ABZ$, analoge Definitionen gelten für $\triangle BCZ$ und $\triangle CAZ$. Dann gilt:

$$n_b^{ABZ} = 3 + b_a + b_b + k_{AB}$$

$$n_b^{BCZ} = 3 + b_b + b_c + k_{BC}$$

$$n_b^{CAZ} = 3 + b_c + b_a + k_{CA}$$

$$n_b = k_{AB} + k_{BC} + k_{CA} + 3$$

$$n_i = 1 + b_A + b_B + b_C + n_i^{ABZ} + n_i^{BCZ} + n_i^{CAZ}$$

Es folgt also:

$$\begin{aligned} & n_b/2 + n_i \\ &= k_{AB}/2 + k_{BC}/2 + k_{CA}/2 + 3/2 \\ & \quad + 1 + b_A + b_B + b_C + n_i^{ABZ} + n_i^{BCZ} + n_i^{CAZ} \\ &= (3 + b_A + b_B + k_{AB})/2 + (3 + b_B + b_C + k_{BC})/2 \\ & \quad + (3 + b_C + b_A + k_{CA})/2 + \left(n_i^{ABZ} + n_i^{BCZ} + n_i^{CAZ} \right) - 2 \end{aligned}$$

$$\begin{aligned}
&= \left(n_b^{ABZ} / 2 + n_i^{ABZ} \right) + \left(n_b^{BCZ} / 2 + n_i^{BCZ} \right) \\
&\quad + \left(n_b^{CAZ} / 2 + n_i^{CAZ} \right) - 2
\end{aligned}$$

Hieraus sehen wir, dass alle drei Dreiecke $\triangle ABZ$, $\triangle BCZ$ und $\triangle CAZ$ die Induktionshypothese erfüllen (d.h. die halbe Anzahl der Gitterpunkte am Rand plus die Anzahl der Gitterpunkte im Inneren ist kleiner als bei $\triangle ABC$). Es folgt:

$$\begin{aligned}
&A(P) \\
&= A(\triangle ABZ) + A(\triangle BCZ) + A(\triangle CAZ) \\
&= \left(n_b^{ABZ} / 2 + n_i^{ABZ} - 1 \right) + \left(n_b^{BCZ} / 2 + n_i^{BCZ} - 1 \right) + \left(n_b^{CAZ} / 2 + n_i^{CAZ} - 1 \right) \\
&= n_b / 2 + n_i - 1
\end{aligned}$$

Fall $m = 3, n_b / 2 + n_i > 3/2, n_i = 0$: Seien A, B und C die Eckpunkte von P . Es muss, da $n_b > 3$ ist auch noch mindestens einen weiteren Gitterpunkt Z auf dem Rand von $\triangle ABC$ geben. Ohne Beschränkung der Allgemeinheit liege Z auf AB . Wir teilen $\triangle ABC$ nun in $\triangle AZC$ und $\triangle ZBC$ und verfahren dann analog zum vorhergehenden Fall.

Fall $m \geq 3$: Wir benutzen Proposition 127 und verfahren dann analog zu den beiden vorhergehenden Fällen. \square

Bemerkung 129. Es ist möglich, die eulersche Formel durch den Satz von Pick zu beweisen. Dafür schaut man sich den dazugehörigen planaren Graphen an, den man so einbettet, dass alle Knoten in dem Gitter \mathbb{Z}^2 liegen. Man erhält eine Fläche die aus $|F| - 1$ kleineren Flächen zusammengesetzt ist. Nun berechnet man den Flächeninhalt einmal direkt und einmal über die $|F| - 1$ kleineren Flächen, beides mal mit dem Satz von Pick. Vergleichen der Formeln ergibt letztlich die eulersche Formel.

Bei dieser Beweismethode ist es allerdings notwendig, zusätzlich zu beweisen, dass $|F|$ unabhängig von der Einbettung ist.

3.3 Der grosse Satz von Fermat

Dieser Abschnitt folgt [9].

Der grosse Satz von Fermat ist folgende, leicht zu formulierende Aussage:

Satz 130. Sei $n > 2$ eine natürliche Zahl. Dann hat die Gleichung

$$x^n + y^n = z^n$$

keine Lösung in positiven ganzen Zahlen.

Fermat schrieb diese Behauptung in die Seitenspalte seiner Kopie des Buchs *Arithmetica* von Diophant (drittes Jahrhundert), mit dem Zusatz, er habe „hierfür einen wahrhaft wunderbaren Beweis entdeckt, doch ist dieser Rand hier zu schmal, um ihn zu fassen“ [8, Seite 3, II].

Bewiesen wurde der grosse Satz von Fermat schliesslich im Jahr 1995 von Andrew Wiles [20]. Obwohl die Aussage des grossen Satzes von Fermat elementarer Form ist, verwendet Wiles Beweis komplexe Techniken aus der algebraischen Geometrie und Zahlentheorie, die viel Theorie voraussetzen.

Eine bisher unbewiesene Vermutung, deren Aussage ebenfalls elementar ist, ist die sogenannte *abc*-Vermutung. Es ist wahrscheinlich, dass diese Aussage ebenfalls keinen einfachen, elementaren Beweis zulässt. Allerdings gibt es einen elementaren Zusammenhang zwischen den beiden Aussagen: Sofern wir die *abc*-Vermutung als wahr annehmen, können wir damit den grossen Satz von Fermat (bzw. eine Variante davon) mittels elementarer Methoden beweisen. Darum soll es in diesem Abschnitt gehen.

Wir werden zunächst polynomielle Formen des Satzes von Fermat und der *abc*-Vermutung beweisen, dann die allgemeine Fassung der *abc*-Vermutung angeben, und schlussendlich einen Teil des grossen Satzes von Fermat aus der *abc*-Vermutung herleiten.

3.3.1 Der grosse Satz von Fermat für Polynome

Definition 131. Ein Polynom in einer Variable t mit Koeffizienten in \mathbb{C} ist eine formale Summe der Form

$$P = \sum_{i=0}^{\infty} a_i t^i$$

mit $a_i \in \mathbb{C}$, wobei nur endlich viele a_i ungleich 0 sein dürfen. Der *Grad* des Polynoms P , für den wir die Notation $\deg(P)$ verwenden, ist der grösste Wert für i , für den $a_i \neq 0$ gilt. Die leere Summe ist ebenfalls erlaubt, wodurch wir das Polynom $P = 0$ erhalten, mit Grad $\deg(0) = -\infty$. Ein konstantes Polynom ist ein Polynom P mit $\deg(P) \leq 0$.

Die Menge aller Polynome in t mit Koeffizienten in \mathbb{C} bezeichnen wir mit $\mathbb{C}[t]$. Es ist möglich Polynome wie gewohnt zu addieren und zu multiplizieren. Darüber hinaus kann die *formale Ableitung* gebildet werden:

$$\frac{d}{dt} \left(\sum_{i=0}^d a_i t^i \right) = \sum_{i=0}^d i a_i t^{i-1} \quad \square$$

Die soeben definierten Operationen auf Polynomen haben einige Eigenschaften, die wir in folgender Proposition festhalten.

Proposition 132. Seien $P, Q \in \mathbb{C}[t]$ und $c \in \mathbb{C} \setminus \{0\}$ (aufgefasst als konstantes Polynom). Dann gilt:

$$\begin{aligned} \deg(P + Q) &\leq \max(\deg(P), \deg(Q)) \\ \deg(c \cdot P) &= \deg(P) \\ \deg(P \cdot Q) &= \deg(P) + \deg(Q) \\ \frac{dP+Q}{dt} &= \frac{dP}{dt} + \frac{dQ}{dt} \\ \frac{dP \cdot Q}{dt} &= P \cdot \frac{dQ}{dt} + \frac{dP}{dt} \cdot Q \end{aligned}$$

Falls $\frac{dP}{dt} = 0$ ist, so ist P ein konstantes Polynom.

Beweis. Wir beweisen nur $\frac{dP \cdot Q}{dt} = P \cdot \frac{dQ}{dt} + \frac{dP}{dt} \cdot Q$. Aufgrund der Kompatibilität beider Seiten der zu zeigenden Gleichung mit Summen in P bzw. Q genügt es, die Aussage für *Monome* zu zeigen, also Polynome der Form $P = c_P t^{d_P}, Q = c_Q t^{d_Q}$ für $d_P, d_Q \in \mathbb{N}$ und $c_P, c_Q \in \mathbb{C}$. Wir erhalten dann:

$$\begin{aligned} P \cdot \frac{dQ}{dt} + \frac{dP}{dt} \cdot Q &= (c_P t^{d_P}) \cdot (d_Q c_Q t^{d_Q-1}) + (d_P c_P t^{d_P-1}) \cdot (c_Q t^{d_Q}) \\ &= d_Q (c_P c_Q t^{d_P+d_Q-1}) + d_P (c_P c_Q t^{d_P+d_Q-1}) = (d_P + d_Q) c_P c_Q t^{d_P+d_Q-1} \\ &= \frac{d}{dt} (c_P c_Q t^{d_P+d_Q}) = \frac{dP \cdot Q}{dt} \quad \square \end{aligned}$$

Proposition 133. Seien $P, Q \in \mathbb{C}[t]$ Polynome, die $P \frac{dQ}{dt} = Q \frac{dP}{dt}$ erfüllen. Dann ist $PQ = 0$ oder es gibt ein $c \in \mathbb{C} \setminus 0$ mit $P = cQ$.

Beweis. Wir beweisen per Induktion über $\max(\deg(P), \deg(Q))$. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass $\deg(P) \geq \deg(Q)$. Falls $Q = 0$ sind wir fertig. Andernfalls sei a der Leitkoeffizient von P und b der Leitkoeffizient von Q . Sei $c = a/b$ (da $Q \neq 0$ ist $b \neq 0$). Dann ist $\deg(P - cQ) < \deg(P)$ und es gilt

$$Q \frac{dP - cQ}{dt} = Q \frac{dP}{dt} - cQ \frac{dQ}{dt} = P \frac{dQ}{dt} - cQ \frac{dQ}{dt} = (P - cQ) \frac{dQ}{dt}$$

Wir können also die Induktionsvoraussetzung anwenden. Falls $P - cQ = 0$, so sind wir wieder fertig, andernfalls gibt es ein $c' \in \mathbb{C}$ mit $P - cQ = c'Q$ und damit $P = (c' + c)Q$. \square

Wir kommen nun zum Hauptergebnis dieses Unterabschnitts.

Satz 134 (Der grosse Satz von Fermat für Polynome). Sei $n \geq 3$ eine natürliche Zahl und $X, Y, Z \in \mathbb{C}[t]$ drei Polynome, die die Gleichung

$$X^n + Y^n = Z^n \tag{3.3.1}$$

erfüllen. Dann gibt es $x, y, z \in \mathbb{C}$, mit $x^n + y^n = z^n$ und ein Polynom $P \in \mathbb{C}[t]$, welches $X = x \cdot P, Y = y \cdot P$ und $Z = z \cdot P$ erfüllt.

Beweis. Sei (X, Y, Z) ein Tupel von Polynomen $X, Y, Z \in \mathbb{C}[t]$, welche 3.3.1 lösen.

Reduktion auf teilerfremde Polynome: Falls es ein nicht-konstantes Polynom Q gibt, für das $X = QX', Y = QY'$ und $Z = QZ'$ gilt, so ist (X', Y', Z') ebenfalls eine Lösung für die Gleichung. Falls für X', Y', Z' die zu zeigende Konklusion gilt, so folgt diese auch für X, Y, Z . Wir können also ohne Beschränkung der Allgemeinheit annehmen, dass X, Y und Z keine gemeinsamen nicht-konstanten Teiler haben. Man bemerke hierbei, dass durch eq. (3.3.1) X, Y, Z auch paarweise schon keine gemeinsamen nicht-konstanten Teiler haben können, und dies der Fall wäre, sollte eines der drei Polynome das Nullpolynom sein.

Einleitung Widerspruchsbeweis: Wir beweisen nun durch Widerspruch und nehmen an, dass X, Y und Z nicht alle konstant sind. Wären zwei dieser drei Polynome konstant, so müsste wegen $X^n + Y^n = Z^n$ auch das dritte konstant sein, also kann dann höchstens eines konstant sein.

Gleichungen die eine Lösung erfüllen muss: Wir bilden die Ableitung von eq. (3.3.1) und erhalten:

$$nX^{n-1} \frac{dX}{dt} + nY^{n-1} \frac{dY}{dt} = nZ^{n-1} \frac{dZ}{dt}$$

Diese Gleichung muss also ebenfalls von (X, Y, Z) erfüllt werden. Nach Teilen durch n erhalten wir:

$$X^{n-1} \frac{dX}{dt} + Y^{n-1} \frac{dY}{dt} = Z^{n-1} \frac{dZ}{dt} \quad (3.3.2)$$

Wir ziehen nun Y mal (3.3.2) von $\frac{dY}{dt}$ mal eq. (3.3.1) ab und erhalten:

$$X^{n-1} \left(X \frac{dY}{dt} - \frac{dX}{dt} Y \right) = Z^{n-1} \left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y \right)$$

Analog lässt sich auch X oder Z eliminieren, wodurch wir zwei weitere Gleichungen obiger Form erhalten.

$\left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y \right)$ ist nicht 0: Falls doch würde aus Proposition 133 folgen, dass wir in einem der folgenden drei Fälle sind:

- (i) Eines der beiden Polynome Y und Z ist das Nullpolynom. Dies haben wir aber schon ausgeschlossen, da die anderen beiden Polynome dann einen gemeinsamen nicht-konstanten Teiler hätten.
- (ii) Y und Z sind beide konstant. Dann wäre aber auch X konstant, im Widerspruch zur Annahme mit dem wir den Widerspruchsbeweis eingeleitet haben.
- (iii) Y und Z haben einen gemeinsamen nicht-konstanten Teiler. Dies hatten wir allerdings zu Beginn ausgeschlossen.

Im Folgenden können wir also annehmen, dass $\left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y\right) \neq 0$.

Teilbarkeitsrelation: Da X und Z keine gemeinsamen nicht-konstanten Teiler haben und $\left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y\right) \neq 0$, folgt, dass sich $\left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y\right)$ als Produkt von X^{n-1} mit einem weiteren Polynom schreiben lässt, genauer gesagt mit

$$Q = \left(X \frac{dY}{dt} - \frac{dX}{dt} Y\right) / Z^{n-1}$$

Folgerung für die Grade der Polynome: Aus

$$0 \neq \left(Z \frac{dY}{dt} - \frac{dZ}{dt} Y\right) = QX^{n-1}$$

folgt, indem wir den Grad beider Seiten berechnen und $\deg(Q) \geq 0$ verwenden:

$$\begin{aligned} (n-1) \deg(X) &\leq \max(\deg(Z) + (\deg(Y) - 1), (\deg(Z) - 1) + \deg(Y)) \\ &= \deg(Y) + \deg(Z) - 1 < \deg(Y) + \deg(Z) \end{aligned}$$

Sofern wir noch $\deg(X)$ zu beiden Seiten hinzuaddieren, erhalten wir eine symmetrischere Form:

$$n \deg(X) < \deg(X) + \deg(Y) + \deg(Z)$$

Analog lässt sich eine solche Ungleichung mit Y oder Z auf der linken Seite erhalten:

$$n \deg(Y) < \deg(X) + \deg(Y) + \deg(Z)$$

$$n \deg(Z) < \deg(X) + \deg(Y) + \deg(Z)$$

Konklusion: Die Summe der eben erhaltenen drei Ungleichungen ist

$$n (\deg(X) + \deg(Y) + \deg(Z)) < 3 (\deg(X) + \deg(Y) + \deg(Z))$$

Nach Annahme ist keines der Polynome 0 und es sind nicht alle konstant, also ist die Summe der Grade positiv. Es folgt also $n < 3$. \square

Bemerkung 135. Die Gleichung

$$(2t)^2 + (t^2 - 1)^2 = (t^2 + 1)^2$$

zeigt, dass sich das Theorem nicht auf $n = 2$ ausweiten lässt.

3.3.2 *abc*-Vermutung für Polynome

Wir kommen nun zu einer ähnlich elementaren Aussage für Polynome, die sich ebenfalls elementar beweisen lässt:

Satz 136. Seien $A, B, C \in \mathbb{C}[t]$ Polynome, die die Gleichung $A + B = C$ erfüllen. Wir nehmen weiterhin an, dass die Polynome nicht alle konstant sind und keine gemeinsamen Nullstellen haben. Sei m die Zahl der verschiedenen Nullstellen von $A \cdot B \cdot C$. Dann gilt

$$\max(\deg(A), \deg(B), \deg(C)) < m$$

Beweis. Wir bemerken zunächst, dass aus der Gleichung ein Widerspruch zu unserer Annahme folgt, sobald schon zwei der drei Polynome konstant sind oder eine gemeinsame Nullstelle haben.

Wir leiten wieder ab und erhalten die Gleichung

$$\frac{dA}{dt} + \frac{dB}{dt} = \frac{dC}{dt}$$

Wir definieren nun

$$\Delta = A \frac{dB}{dt} - \frac{dA}{dt} B$$

und bemerken, dass dann

$$\begin{aligned} \Delta &= A \left(\frac{dC}{dt} - \frac{dA}{dt} \right) - \frac{dA}{dt} (C - A) \\ &= A \frac{dC}{dt} - A \frac{dA}{dt} - \frac{dA}{dt} C + A \frac{dA}{dt} \\ &= A \frac{dC}{dt} - \frac{dA}{dt} C \end{aligned}$$

Analog erhalten wir auch

$$\Delta = C \frac{dB}{dt} - B \frac{dC}{dt}$$

Mit dem gleichen Argument wie bei dem grossen Satz von Fermat lässt sich zeigen, dass $\Delta \neq 0$.

Sei nun α eine Nullstelle von A der Ordnung/Vielfachheit e , sodass also $(t - \alpha)^e$ dann A teilt.

Die Ableitung $\frac{dA}{dt}$ hat an α eine Nullstelle der Ordnung $e - 1$, sodass Δ an α eine Nullstelle der Ordnung mindestens $e - 1$ hat. Es folgt, dass $(t - \alpha)^e$ ein Teiler von $\Delta \cdot (t - \alpha)$ ist. Sofern wir dies für alle Nullstellen von A, B und C wiederholen (und verwenden, dass diese drei Polynome keine gemeinsamen Nullstellen haben), so erhalten wir², dass ABC ein Teiler von $\Delta \cdot \prod_{(A \cdot B \cdot C)(\alpha)=0} (t - \alpha)$ ist.

²Wir benutzen an dieser Stelle auch den Fundamentalsatz der Algebra

Da $\Delta \neq 0$ erhalten wir für die Grade:

$$\deg(A) + \deg(B) + \deg(C) \leq \deg(\Delta) + m \quad (3.3.3)$$

Aus den Gleichungen für Δ erhalten wir

$$\deg(\Delta) \leq \deg(A) + \deg(B) - 1 = (\deg(A) + \deg(B) + \deg(C)) - \deg(C) - 1$$

und analoge Ungleichungen mit $-\deg(B)$ bzw. $-\deg(A)$. Es folgt also

$$\deg(\Delta) \leq (\deg(A) + \deg(B) + \deg(C)) - \max(\deg(A), \deg(B), \deg(C)) - 1$$

Damit folgt aus eq. (3.3.3) durch Subtraktion von

$$\deg(A) + \deg(B) + \deg(C) - \max(\deg(A), \deg(B), \deg(C))$$

auf beiden Seiten

$$\max(\deg(A), \deg(B), \deg(C)) \leq m - 1 < m$$

□

3.3.3 Von abc zu Fermat (für Polynome)

Aus Theorem 136 lässt sich leicht Theorem 134 folgern:

Wir behalten die Notation der beiden Theoreme bei und definieren $A = X^n$, $B = Y^n$ und $C = Z^n$. Laut Theorem 136 ist dann

$$\max(\deg(A), \deg(B), \deg(C)) < m$$

wobei m die Zahl der verschiedenen Nullstellen von $A \cdot B \cdot C$ ist.

Wir bemerken nun zunächst, dass $ABC = (XYZ)^n$ genausoviele verschiedene Nullstellen hat wie XYZ . Desweiteren hat XYZ höchstens $\deg(XYZ)$ viele Nullstellen, woraus folgende Ungleichung folgt.

$$m \leq \deg(X) + \deg(Y) + \deg(Z) \leq 3 \max(\deg(X), \deg(Y), \deg(Z))$$

Ausserdem ist $\deg(A) = \deg(X^n) = n \deg(X)$ und analog für B und C . Kombinieren der beiden Ungleichungen ergibt dann:

$$\begin{aligned} n \cdot \max(\deg(X), \deg(Y), \deg(Z)) &< 3 \max(\deg(X), \deg(Y), \deg(Z)) \\ \Rightarrow n &< 3 \end{aligned}$$

3.3.4 Die abc -Vermutung

Wir haben nun gesehen, wie sich das Analogon des grossen Satzes von Fermat für Polynome aus der abc -Vermutung für Polynome³ herleiten lässt. Wir würden gerne eine Variante der abc -Vermutung finden, mit deren Hilfe sich der grosse Satz von Fermat auch in seiner Fassung für ganze Zahlen, also wie in Theorem 130 angeben, beweisen lässt.

Seien also a, b, c positive ganze Zahlen, die $a + b = c$ erfüllen. Die kleinsten Teiler von Polynomen in \mathbb{C} waren der Form $t - \alpha$, für eine Nullstelle α . Für ganze Zahlen ist es dann naheliegend, die Faktorisierung in Primzahlen zu betrachten. Die Anzahl der verschiedenen Nullstellen von ABC entspricht also die Anzahl der Primzahlen, die abc teilen. Dies können wir schreiben als $\sum_{p \text{ prim}, p|abc} 1$. Die Primfaktorzerlegung einer positiven ganzen Zahl x können wir schreiben als

$$x = \prod_{p \text{ prim}} p^{e_p(x)}$$

Das naheliegende Analogon zum Grad eines Polynoms ist dann $\sum_{p \text{ prim}} e_p(x)$. In Analogie zu Theorem 136 könnten wir also die Vermutung aufstellen, dass

$$\max \left(\sum_{p \text{ prim}} e_p(a), \sum_{p \text{ prim}} e_p(b), \sum_{p \text{ prim}} e_p(c) \right) < \sum_{p \text{ prim}, p|abc} 1$$

Leider ist diese Vermutung nicht richtig, $1 + 1 = 2$, $1 + 3 = 4$ oder $1 + 8 = 9$ sind Gegenbeispiele.

Eine erste Korrektur können wir vornehmen, indem wir berücksichtigen, dass verschiedene Primzahlen in unseren Zählungen unterschiedlich gewichtet werden sollten. In der Zahlentheorie hat sich vielfach bewährt, Primzahlen mit ihrem Logarithmus zu gewichten. Wir erhalten dann also als neuen Versuch:

$$\max \left(\sum_{p \text{ prim}} e_p(a) \log(p), \sum_{p \text{ prim}} e_p(b) \log(p), \sum_{p \text{ prim}} e_p(c) \log(p) \right) < \sum_{p \text{ prim}, p|abc} \log(p)$$

Da $\exp \left(\sum_{p \text{ prim}} e_p(x) \log(p) \right) = \prod_{p \text{ prim}} p^{e_p(x)} = x$ ist, erhalten wir nach Anwendung von $\exp(-)$ auf diese Ungleichung:

$$\max(a, b, c) < \prod_{p \text{ prim}, p|abc} p$$

³ welche allerdings keine Vermutung ist, da wir sie bewiesen haben.

Da $a + b = c$ und alle drei positive ganze Zahlen sind ist $\max(a, b, c) = c$. Schlussendlich erhalten wir also die Formulierung

$$c < \prod_{p \text{ prim, } p|abc} p$$

Diese Vermutung stellt sich allerdings ebenfalls als falsch heraus: $1 + 8 = 9$ oder $5 + 27 = 32$ sind etwa Gegenbeispiele.

Die zuletzt erhaltene Formulierung ist allerdings schon nahe an der Vermutung von Oesterl und Masser:

Vermutung 137 (*abc*-Vermutung). Für jede positive reelle Zahl ϵ gibt es eine Konstante K_ϵ derart, dass für jedes Tripel von positiven ganzen Zahlen (a, b, c) ohne gemeinsame Teiler, die die Gleichung $a + b = c$ erfüllen, gilt:

$$c < K_\epsilon \cdot \left(\prod_{p \text{ prim, } p|abc} p \right)^{1+\epsilon}$$

Eine konkretere Vermutung ist, dass obige Ungleichung für $\epsilon = 1$ und $K_1 = 1$ erfüllt ist.

Vermutung 138. Für jedes Tripel von positiven ganzen Zahlen (a, b, c) ohne gemeinsame Teiler, die die Gleichung $a + b = c$ erfüllen, gilt:

$$c < \left(\prod_{p \text{ prim, } p|abc} p \right)^2$$

3.3.5 Von der *abc*-Vermutung zum grossen Satz von Fermat

Satz 139. Sei $n > 5$ eine natürliche Zahl. Dann hat die Gleichung

$$x^n + y^n = z^n$$

keine Lösung in positiven ganzen Zahlen, unter Annahme von Vermutung 138.

Beweis. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass x, y und z paarweise teilerfremd sind.

Nach Vermutung 138 angewendet auf $a = x^n, b = y^n, c = z^n$ gilt dann:

$$z^n < \left(\prod_{p \text{ prim, } p|x^n y^n z^n} p \right)^2$$

Eine Primzahl teilt $x^n y^n z^n$ genau dann, wenn sie xyz teilt. Also erhalten wir

$$\begin{aligned} \left(\prod_{p \text{ prim, } p|x^n y^n z^n} p \right)^2 &= \left(\prod_{p \text{ prim, } p|xyz} p \right)^2 \\ &\leq (xyz)^2 \leq (z^3)^2 = z^6 \end{aligned}$$

Indem wir nun auf die kombinierte Ungleichung den Logarithmus zur Basis z anwenden (es ist $z > 1$, da $z \in \mathbb{Z}_{>0}$ und $x^n + y^n = 1^n$ nicht möglich ist für $x, y \in \mathbb{Z}_{>0}$) erhalten wir:

$$n < 6$$

3.3.6 Ein Beweis des grossen Satzes von Fermat für $n = 4$

In diesem Unterabschnitt geben wir einen von den bisherigen Ergebnissen unabhängigen Beweis einer leichten Verallgemeinerung des grossen Satzes von Fermat für den Exponenten $n = 4$. Wir werden dabei die folgenden beiden Aussagen verwenden, die sich ebenfalls elementar beweisen lassen:

Proposition 140 ([5, Lemma 12.1]). Seien a, b, c teilerfremde positive ganze Zahlen mit

$$a^2 + b^2 = c^2$$

Dann ist genau eine der beiden Zahlen a und b gerade.

Satz 141 ([5, Theorem 12.1]). Seien a, b, c teilerfremde positive ganze Zahlen mit

$$a^2 + b^2 = c^2$$

und $2|a$. Dann gibt es teilerfremde positive ganze Zahlen $m > n$, von denen genau eine gerade ist und so, dass die Gleichungen

$$a = 2mn, b = m^2 - n^2, c = m^2 + n^2$$

erfüllt sind.

Satz 142 ([5, Theorem 12.3]). Es gibt keine ganzzahligen Lösungen der Gleichung $x^4 + y^4 = z^2$.

Beweis. Zunächst können wir jede Variable durch ihren Betrag ersetzen, es genügt also nichtnegative Lösungen zu betrachten. Weiterhin genügt es analog zu den anderen Beweisen in diesem Abschnitt, paarweise teilerfremde Lösungen zu betrachten. Sei dann (x, y, z) unter den nicht-negativen ganzzahligen und paarweise teilerfremden Lösungen die, bei der z minimal ist.

Setzen wir $a = x^2$, $b = y^2$ und $c = z$, so folgt aus Proposition 140, dass genau eine der beiden Zahlen x und y gerade ist. Wir können ohne Beschränkung der Allgemeinheit annehmen, dass x gerade ist. Dann können wir Theorem 141 anwenden und erhalten teilerfremde positive ganze Zahlen $m > n$ von denen genau eine gerade ist mit

$$x^2 = 2mn, y^2 = m^2 - n^2, z = m^2 + n^2$$

Quadrate von ungeraden Zahlen haben modulo 4 den Rest 1 und gerade Zahlen den Rest 0. Also hat y^2 modulo 4 den Rest 1 und von m und n muss m die ungerade Zahl sein und n die gerade (ansonsten wäre der Rest modulo 4 stattdessen 3).

Wir schreiben nun $n = 2r$ und erhalten $(x/2)^2 = mr$. Da ein Produkt von teilerfremden Zahlen nur dann ein Quadrat sein kann, wenn die beiden Faktoren schon Quadrate sind, folgt, dass es positive ganze Zahlen z' und w gibt mit $m = (z')^2$ und $r = w^2$.

Durch umstellen von $y^2 = m^2 - n^2$ erhalten wir $n^2 + y^2 = m^2$. Da n gerade ist und n und m teilerfremd sind die Voraussetzungen an Theorem 141 erfüllt und wir erhalten teilerfremde positive ganze Zahlen $u > v$ mit

$$n = 2uv, y = u^2 - v^2, m = u^2 + v^2$$

Es ist also $uv = t/2 = r = w^2$ folglich müssen erneut auch u und v Quadrate sein. Es gibt also positive ganze Zahlen x' und y' mit $u = (x')^2$ und $v = (y')^2$.

Es folgt damit

$$(z')^2 = m = u^2 + v^2 = (x')^4 + (y')^4$$

Da x' und y' teilerfremd sind haben wir also eine weitere Lösung (x', y', z') der betrachteten Gleichung gefunden. Es gilt allerdings auch, da $z', m, n \geq 1$:

$$0 < z' \leq (z')^2 = m \leq m^2 < m^2 + n^2 = z$$

Dies widerspricht der Annahme, dass (x, y, z) eine Lösung mit minimalem z ist. \square

Literaturverzeichnis

- [1] Actualitix, *Carte de la Bretagne*. <https://www.actualitix.com/carte-bretagne.html>.
- [2] Aigner, M. und Ziegler, G. M. *Raisonnements divins*, Springer Verlag France, 2013.
- [3] Bankov, K., *Applications of the Pigeon-Hole Principle*, The Mathematical Gazette 79 (485), pp. 286–292, 1995.
- [4] Bova, C. und Di Filippo, C. und Gigliotti, P. und Alfieri, A., *Cathedrals, houses and blue poles* Presentation. Liceo Scientifico L. Siciliani Catanzaro Fractals and art European Student Conference in Mathematics EUROMATH, 2012.
- [5] Burton, D. M., *Elementary Number Theory*, 6th edition, McGraw-Hill, 2007.
- [6] Derksen, H., *Problem set 7: pigeon hole principle*, <http://www.math.lsa.umich.edu/~hderksen/ProblemSolving/PS7.pdf>.
- [7] Falconer, K., *Fractal Geometry: Mathematical Foundations and Applications*. Wiley-Blackwell, 2003.
- [8] Fermat, P. de, und Miller, M., *Bemerkungen zu Diophant*, Leipzig : Akademische Verlagsgesellschaft m. b. h, <https://trove.nla.gov.au/work/22233849>, 1932.
- [9] Granville, A., und Tucker, T. J., *It's as easy as abc*, Notices of the AMS 49 (10), pp. 1224–1231, 2002.
- [10] Mandelbrot, B., *How long is the coast of Britain? Statistical self-similarity and fractional dimension*, Science 156 (3775), pp. 636–638, 1967.
- [11] Meisters, G. H., *Polygons Have Ears*, The American Mathematical Monthly 82 (6), pp. 648–651, 1975.
- [12] Meyer, B., *Graphes, formules d'Euler et solides de Platon*. http://paestel.fr/sites/default/files/Mat_les_ressources/Terminale/Atelier.
- [13] Nahin, P. J., *Inside Interesting Integrals*, Undergraduate Lecture Notes in Physics, Springer, New York, NY, 2014.
- [14] Niven, I., *Irrational Numbers*, Carus Mathematical Monographs (Book 11), The Mathematical Association of America, 2005.

- [15] Riter, P., *Petit recueil d'énigmes*, http://www.univ-orleans.fr/mapmo/membres/cordier/centre-galois/doc/ENIGMES_AVEC_SOL.pdf.
- [16] Rouget, J.-L., *Exo 7 Topologie*, <http://exo7.emath.fr/ficpdf/fic00134.pdf>.
- [17] RRL, *An application of the pigeonhole principle in analysis*, <https://math.stackexchange.com/questions/2282584/an-application-of-the-pigeonhole-principle-in-analysis/2282655>.
- [18] Trevor, B. und Shenoy, V. und Gaba, P. et al., *Integration Tricks*, <https://brilliant.org/wiki/integration-tricks/>.
- [19] Wikipedia, *Hall's marriage theorem*, <https://en.wikipedia.org/wiki/Hall>.
- [20] Wiles, A., *Modular Elliptic Curves and Fermat's Last Theorem*, *Annals of Mathematics* 141 (3), pp. 443–551, 1995.