

# 1 Théorie

## 1.1 Fraction continues

### 1.1.1 Intuition

Intuitivement, une fraction continue est une expression — finie ou infinie — de la forme suivante<sup>1</sup> :

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

telle que  $a_0 \in \mathbb{Z}$  et  $a_i \in \mathbb{N}^*$  pour tout  $i \in \mathbb{N}^*$ . Toujours intuitivement, nous voulons affûbler cette fraction continue d'une valeur. Si la fraction continue est finie, cette est une bonne vieille fraction, c'est à dire un élément du corps  $\mathbb{Q}$  ; si la fraction continue est infinie, on calcule d'abord  $a_0$ , puis  $a_0 + \frac{1}{a_1}$ , puis  $a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$ , et on continue une infinité de fois. La limite de la suite générée est la « valeur » de la fraction continue. Nous ferons sens plus précis de l'intuition dans la prochaine sous-section.

Les fractions continues émanent de la volonté d'approcher des réels irrationnels par des fractions d'entiers. Par exemple, la fraction  $\frac{103993}{33102}$  approche  $\pi$  avec une précision meilleure que le milliardième. Comment générer une telle fraction continue pour un réel irrationnel  $x$  ? On part de l'identité  $x = x + [x] - [x]$  et l'on écrit

$$x = [x] + \frac{1}{\frac{1}{x - [x]}}.$$

On pose  $x_0 = x$  et  $x_1 = \frac{1}{x_0 - [x_0]}$  (qui est bien défini par irrationalité de  $x$ ) et l'on répète la première étape sur  $x_1$  :

$$x = [x_0] + \frac{1}{x_1} = [x_0] + \frac{1}{[x_1] + \frac{1}{\frac{1}{x_1 - [x_1]}}}.$$

Comme le réel  $x$  est irrationnel, on peut répéter ce procédé indéfiniment. Nous construisons alors la suite d'éléments *irrationnels* de terme général

$$x_n = \frac{1}{x_{n-1} - [x_{n-1}]}, \quad \forall n \geq 1.$$

---

1. Notez que nous ne nous autorisons que des 1 aux numérateurs.

On associe alors à l'irrationnel  $x$  la fraction continue *infinie*<sup>2</sup>

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}},$$

où l'on a posé

$$a_i = \lfloor x_i \rfloor$$

pour tout  $i \in \mathbb{N}$ . Fixons ces notations :

**Notation 1.1.** Soit  $x \in \mathbb{R}$  un élément irrationnel. Notons  $x_0 = x$  puis

$$x_n := \frac{1}{x_{n-1} - \lfloor x_n \rfloor}, \quad \forall n \geq 1.$$

Par ailleurs, notons

$$\hat{x}_n := \lfloor x_n \rfloor, \quad \forall n \in \mathbb{N}.$$

**Remarque 1.2.** La méthode de construction d'une fraction continue *finie* pour un rationnel est la même : il faut simplement s'arrêter lorsque l'on tombe sur un  $a_n$  vérifiant  $a_n = \lfloor a_n \rfloor$ . Cet algorithme termine (**ref**) et s'exécute plus simplement en utilisant... l'algorithme d'Euclide. Par ailleurs, réaffirmons que la fraction continue d'un irrationnel (encore une fois, dans un sens qui sera précisé au prochain paragraphe) est forcément infinie.

### 1.1.2 Formalisation

Formellement, on peut définir<sup>3</sup> une fraction continue ainsi :

**Définition 1.3** (Fraction continue). On appelle *fraction continue* toute suite non vide (finie ou infinie)  $(a_i)_{i \in U} \in \mathbb{N}^{\mathbb{N}}$ ,  $U \subset \mathbb{N}$ , d'entiers qui vérifie

$$a_i \geq 1, \quad \forall i \in U \setminus \{0\}.$$

Cette suite est alors notée

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}.$$

---

2. Lorsque nous aurons correctement défini la notion de fraction continue, cette fraction continue canoniquement associée à  $x$  sera notée  $\hat{x}$ .

3. La définition mathématique est descriptive et non prescriptive.

**Notation 1.4.** Soit  $x \in \mathbb{R}$  un élément irrationnel. On note  $\hat{x}$  la fraction continue infinie canoniquement associée à  $x$  par la méthode exposée dans le premier paragraphe. Autrement dit,  $\hat{x}$  est la fraction continue donnée par la suite infinie (voir 1.1)  $(\hat{x}_i)_{i \in \mathbb{N}}$ .

Il est naturel d'associer à une fraction continue (finie ou infinie) une suite (finie ou infinie) de fractions « intermédiaires » appelées *réduites*. Pour n'avoir aucun problème de division par zéro, nous nous plaçons temporairement dans un corps de fractions rationnelles en  $\mathbb{N}$  indéterminées.

**Définition 1.5** (Réduites formelles). Soit  $(X_i)_{i \in \mathbb{N}}$  une suite (infinie) d'indéterminées sur le corps  $\mathbb{Q}$ . On définit

$$[X_0] = X_0$$

puis par récurrence

$$[X_1, \dots, X_n] = X_0 + \frac{1}{[X_1, \dots, X_n]}.$$

Ces éléments sont dans  $\mathbb{Q}((X_i)_{i \in \mathbb{N}})$ .

**Définition 1.6** (Réduites d'une fraction continue). Distinguons les cas finis et infinis. Soit  $f$  une fraction continue.

- Si  $f$  est donnée par la suite finie  $(a_0, \dots, a_n)$ , pour tout  $k \in \llbracket 0, n \rrbracket$  on appelle  $k$ -ième réduite de  $f$  l'élément  $[a_0, \dots, a_k]$ .
- Si  $f$  est donnée par la suite infinie  $(a_i)_{i \in \mathbb{N}}$ , pour tout  $k \in \mathbb{N}$  on appelle  $k$ -ième réduite de  $f$  l'élément  $[a_0, \dots, a_k]$ .

**Exemple 1.7.** Soit  $f$  la fraction continue infinie donnée par la suite  $(1)_{i \in \mathbb{N}}$ . La première réduite est  $[1] = 1$ , la deuxième est

$$[1, 1] = 1 + \frac{1}{[1]} = 1 + \frac{1}{1},$$

la troisième est

$$[1, 1, 1] = 1 + \frac{1}{[1, 1]} = 1 + \frac{1}{1 + \frac{1}{1}}.$$

Plus généralement, la  $k$ -ième réduite de  $f$  est de la forme

$$[1, 1, \dots, 1] = 1 + \frac{1}{1 + \frac{1}{\dots \frac{1}{1 + \frac{1}{1}}}}.$$

Remarquons que les réduites de toute fraction continue sont des éléments rationnels, ce même si la fraction continue est égale à  $\hat{x}$  pour un certain irrationnel  $x$ . De fait,  $x$  n'est égal à aucune des réduites de  $\hat{x}$ . Les fractions continues finies ne se comportent pas pareil puisque toute fraction continue finie donnée par la suite  $(a_1, \dots, a_n)$  est *égale*<sup>4</sup> à la réduite  $[a_1, \dots, a_n]$ . Toutefois, en reprenant les notations 1.1, on a

$$x = [\hat{x}_1, \dots, \hat{x}_{n-1}, x_n], \quad \forall x \in \mathbb{N}. \quad (1)$$

Cette égalité sera fondamentale dans notre algorithme de factorisation.

Nous donnons à présent un sens à l'égalité entre une fraction continue et un réel. Si la fraction continue est finie, alors elle est en particulier un élément du corps  $\mathbb{Q}$  et il n'y a rien à faire. Nous nous concentrons sur le cas infini.

**Définition 1.8.** Soient  $l$  un réel et  $f$  une fraction continue donnée par la suite infinie  $(a_i)_{i \in \mathbb{N}}$ . On dit que  $f$  est *égale* à  $l$  et l'on note  $f = l$  si la suite des réduits de  $f$  converge vers  $l$ .

**Exemple 1.9** (Nombre d'or). On appelle *nombre d'or* et l'on note  $\varphi$  l'unique racine réelle positive du polynôme  $X^2 - X - 1 \in \mathbb{Z}[X]$ . On a  $\varphi = \frac{1+\sqrt{5}}{2} \simeq 1,618$ . Comme  $\varphi^2 = \varphi + 1$  et que  $\varphi \neq 0$ , on a  $\varphi = 1 + \frac{1}{\varphi} = 1 + \frac{1}{1 + \frac{1}{\varphi}}$ . En réalité,  $\varphi$  est égal à une

fraction continue :

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

### 1.1.3 Irrationnels quadratiques

---

4. Au sens bien connu de l'égalité dans le corps  $\mathbb{Q}$