Caractérisation des singularités de type $\mathfrak{J}$

Félix Larose-Gervais

Mai 2023

Contents

1 Introduction

1.1 Notations

Soit $m, n \in \mathbb{N}$, X un ensemble, notons

- $Sym(X)$ le groupe de bijections de X dans lui-même
- $Sym(m)$ le groupe de bijections $Sym(\{1, \dots, m\})$
- $\mathbb{Z}_n$ l'anneau des entiers modulo n ($\mathbb{Z}/n\mathbb{Z}$)
- $\mathbb{Z}_n^\times$ son groupe d'inversibles ($\{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$)
- X^m les m-uplets de X ($\underbrace{X \times \cdots \times X}_{m fois}$)

On notera aussi S_n^m les m-uplets d'inversibles modulo n (${\mathbb{Z}_n^\times}^m$)

1.2 Définitions

Définition 1. *Une **singularité** est un $[a] = ([a_1], \dots, [a_m]) \in S_n^m$, on appelle*

- *n la **racine** de la singularité*
- *$[a_1], \dots, [a_m]$ les **poids** de la singularité*

Définition 2. *Un **éclatement** $a \in \mathbb{Z}^m$ d'une singularité $[a] \in S_n^m$ (noté $a \in [a]$) est un choix de représentant $a = (a_1, \dots, a_m)$ tel que*

$$\forall i \neq j : \gcd(a_i, a_j) = 1$$

On note E_a l'ensemble des singularités associées à l'éclatement a comme suit:

$$\begin{aligned}
&E_a = \{[a^i] \in S_{a_i}^m \mid \forall i = 1..m,\ a_i > 1\} \\
&[a^i] = ([a_1^i], \dots, [a_m^i]) \\
&[a_j^i] \equiv \begin{cases} -n & si\ i = j \\ a_j & sinon \end{cases} \pmod{a_i} \quad \forall j = 1..m
\end{aligned}$$

*On appelle $a = (a_1, \dots, a_m)$ **l'éclatement naturel** de $[a]$ si les $a_1, \dots, a_m$ sont les plus petits représentant positifs de leurs classes*

Définition 3. *Un éclatement $a \in [a]$ est dit **lisse** si $E_a = \emptyset$*

Définition 4. *La singularité $[a]$ est dite de **type** $\mathfrak{I}$ (noté $[a] \in \mathfrak{I}$) ssi*

$$\exists a \in [a] : \forall [a^i] \in E_a : [a^i] \in \mathfrak{I}$$

1.3 Rappels d'arithmétique

1.3.1 Algorithme d'Euclide et PGCD

Soit $a, b \in \mathbb{Z}$, on calcule le PGCD comme suit

$$\gcd(a,b) := \begin{cases} a & \text{si } b = 0 \\ \gcd(b, a \mod b) & \text{sinon} \end{cases}$$

Avec $k \in \mathbb{Z}$, on a les propriétés suivantes:

$$\gcd(a,1) = 1 \tag{1}$$
$$\gcd(a,b) = \gcd(b,a) \tag{2}$$
$$\gcd(a,b) = \gcd(a+kb,b) \tag{3}$$

De la dernière on déduit directement, pour $n \in \mathbb{N}$

$$a \equiv b \pmod n$$
$$\implies \gcd(a,n) = \gcd(b,n)$$

1.3.2 Théorème des restes chinois

Soit $m, n_1, \ldots, n_m \in \mathbb{N}$ et $a_1, \ldots, a_m \in \mathbb{Z}$, notons le produit $n = n_1 \cdots n_m$

Si $\forall i \neq j : \gcd(n_i, n_j) = 1$

Alors $\exists! x \in \mathbb{Z}_n$ tel que

$$x \equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv a_m \pmod{n_m}$$

1.4 Résultats connus

Résultats utiles, dûs à Habib Jaber.

Proposition 1. *Soit* $a_1, a_2 \in \mathbb{Z},\ \gcd(a_1,a_2) = 1,$ *alors*

$$[(a_1,a_2)]_{a_1+a_2} \in \mathfrak{J}$$

Exemple 1. $\gcd(2,1) = 1 \implies [(2,1)]_3 \in \mathfrak{J}$

Proposition 2.

$$[(a_1,a_2)]_n \in \mathfrak{J} \iff \forall k \in \mathbb{Z} : [(a_1,a_2)]_{n+ka_1a_2} \in \mathfrak{J}$$

Exemple 2. $[(2,1)]_3 \in \mathfrak{J} \implies [(2,1)]_5 \in \mathfrak{J},\ [(2,1)]_7 \in \mathfrak{J}, \ldots$

2 Propositions

Soit $\sigma \in Sym(m)$, et ces permutations associées $\pi_\sigma \in Sym(S_n^m)$

Proposition 3. *L'ordre des poids d'une singularité n'affecte pas le type* $\mathfrak{J}$

$$[a] \in \mathfrak{J} \implies \pi_\sigma([a]) \in \mathfrak{J}$$

Proof. Pour $a = (a_1, \ldots, a_m) \in [a]$ tel que $\forall [a^i] \in E_a : [a^i] \in \mathfrak{J}$, on a

1. Cas de base: $E_a = \emptyset$
   On a donc $a = (1, \ldots, 1)$
   Ainsi $[a] = ([1], \ldots, [1]) = \pi_\sigma([a]) \in \mathfrak{J}$
2. Induction structurelle
   Supposons $\forall [a^i] \in E_a : [a^i] \in \mathfrak{J} \implies \pi_\sigma([a^i]) \in \mathfrak{J}$

$$\begin{aligned} E_a &= \{[a^i] \in S_{a_i}^m \mid \forall i = 1..m,\ a_i > 1\} \\ [a^i] &= ([a_1^i], \ldots, [a_m^i]) \\ [a_j^i] &\equiv \begin{cases} -n & \text{si } i = j \\ a_j & \text{sinon} \end{cases} \pmod{a_i} \quad \forall j = 1..m \end{aligned}$$

   Considérons, pour $b = (b_1, \ldots, b_m) = (a_{\sigma(1)}, \ldots, a_{\sigma(m)}) \in \pi_\sigma([a])$

$$\begin{aligned} E_b &= \{[b^i] \in S_{b_i}^m \mid \forall i = 1..m,\ b_i > 1\} \\ [b^i] &= ([b_1^i], \ldots, [b_m^i]) \\ [b_j^i] &\equiv \begin{cases} -n & \text{si } i = j \\ b_j & \text{sinon} \end{cases} \pmod{b_i} \quad \forall j = 1..m \\ &\equiv \begin{cases} -n & \text{si } \sigma(i) = \sigma(j) \\ a_{\sigma(j)} & \text{sinon} \end{cases} \pmod{a_{\sigma(i)}} \\ &\equiv [a_{\sigma(j)}^{\sigma(i)}] \\ [b^i] &= ([a_{\sigma(1)}^{\sigma(i)}], \ldots, [a_{\sigma(m)}^{\sigma(i)}]) \\ &= \pi_\sigma([a^{\sigma(i)}]) \in \mathfrak{J} \end{aligned}$$

   Ainsi $\pi_\sigma([a]) \in \mathfrak{J}$

$\square$

Exemple 3. *Sachant* $[(3, 2)]_5 \in \mathfrak{J}$, *on en déduit* $[(2, 3)]_5 \in \mathfrak{J}$

Proposition 4. *(strict, rework) Soit $a = (a_0, a_1, a_2)$, alors*

$$a \in \mathfrak{J} \implies a_0 \geq a_1 + a_2$$

Proof. Supposons $a_0 < a_1 + a_2$

Si $a_1 = a_2$, alors $\neg\mathfrak{J}(a)$

Sinon, $a_1 \neq a_2$, supposons sans perdre de généralité que $a_1 > a_2$

Considérons l'éclatement $a^1 = (a_1,\ -a_0 \mod a_1,\ a_2 \mod a_1) \in E_a$

$$\begin{aligned}
a_1 > a_2 &\implies 2a_1 > a_1 + a_2 \\
&\implies (-a_0 \mod a_1) = 2a_1 - a_0 \\
a_1 > a_2 &\implies (a_2 \mod a_1) = a_2
\end{aligned}$$

On a donc $a^1 = (a_1, 2a_1 - a_0, a_2)$

Puisque $a_0 < a_1 + a_2$, on a $a_1 < 2a_1 - a_0 + a_2$

Donc a^1 vérifie la condition initiale, on répète le raisonnement avec a^1 $\square$

Exemple 4. $(5, 4, 3) \notin \mathfrak{J}$ *car* $5 < 7$

Proposition 5. *Toute singularité admet un éclatement*

Proof. Soit $[a] = ([a_1], \ldots, [a_m]) \in S_n^m$

Prenons $(a_1, \ldots, a_m) \in [a]$ son représentant naturel

On cherche $(b_1, \ldots, b_m) \in [a]$ tels que $\forall i \neq j : \gcd(b_i, b_j) = 1$

Il suffit de prendre $b_1 = a_1$ et $\forall i = 2..m$, un b_i vérifiant

$$\begin{aligned}
b_i &\equiv a_i \pmod n \\
b_i &\equiv 1 \pmod{b_1} \\
&\vdots \\
b_i &\equiv 1 \pmod{b_{i-1}}
\end{aligned}$$

De tels b_i existent par le théorème des restes chinois

On vérifie la coprimalité sachant, étant donné $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}$

$$\gcd(a, 1) = 1 \text{ et } a \equiv b \pmod c \implies \gcd(a, c) = \gcd(b, c)$$

On a donc

$$\begin{aligned}
\forall i : \gcd(b_i, n) &= 1 \\
\forall i \neq j : \gcd(b_i, b_j) &= 1
\end{aligned}$$

$\square$

3 Conjectures

Conjecture 1. *Soit* $a = (a_0, a_1, a_2)$ *un éclatement d'une singularité* $[a]$
Posons $s = a_1 + a_2 + \gcd(a_0 - a_1, a_0 - a_2)$
Supposons $a_0 < s$
Alors $[a]$ *est de type* $\mathfrak{J} \implies s = a_0 + 1$

On constate que la réciproque n'est pas vraie, par exemple prenons $(13, 7, 4)$, on a $s = 14$, vérifiant donc $a_0 < 14$ et $a_0 + 1 = 14$, or elle n'est pas de type $\mathfrak{J}$.

Conjecture 2. *Soit* $a = (a_0, a_1, a_2)$ *un éclatement d'une singularité* $[a]$
Alors $[a]$ *est de type* $\mathfrak{J} \implies \exists p, q : a_0 = p * a_1 + q * a_2$

Conjecture 3. *(strict) Soit* $[a] = ([a_1], \ldots, [a_m]) \in \mathfrak{J}, m \geq 2$
Alors $|\{a_i \in [a] \mid a_i == 1\} \geq m - 2$

Conjecture 4. *Si* $[a] \in \mathfrak{J}$*, alors son représentant naturel* $a \in [a]$ *offre une suite d'éclatement montrant* $[a] \in \mathfrak{J}$